राज्यातील विविध शहरांमध्ये सुरक्षिततेच्या दृष्टीकोनातून सीसीटीव्ही संनिरीक्षण यंत्रणा सविस्तर प्रकल्प अहवाल (Detailed Project Report) / विनंती प्रस्ताव (Request For Proposal) बाबत मार्गदर्शक तत्वे विहित करण्याबाबत.

महाराष्ट्र शासन
गृह विभाग
शासन निर्णय क्रमांका सीसीटी-३६२३/प्र.क्र.१२१/पोल-३
मादाम कामा रोड, हुतात्मा राजगुरु चौक,
दुसरा मजला, मंत्रालय, मुंबई-३२.
दिनांक: २५ जानेवारी, २०२४.

वाचा : १) नियोजन शासन निर्णय क्र. डिएपी-१०११/प्र.क्र.१८२/का.१४८१. दि.८ ऑगस्ट, २०११.
२) नियोजन विभाग, शासन निर्णय क्र. स्थाविका-२०११/प्र.क्र.४७/का.१४८२, दि.१३ सप्टेंबर, २०११.
३) गृह विभाग, शासन निर्णय क्र. सीसीटी-३६१५/प्र.क्र.३६/पोल-३, दि.९ जानेवारी, २०१७

प्रस्तावना :

सार्वजनिक सुरक्षितता, कायदा व सुव्यवस्था अबाधित राखणे, अतिरेक्यांच्या कारवाया रोखणे, धार्मिक कार्यक्रम व मिरवणुकांवर नियंत्रण ठेवणे, वाहतुकीचे नियंत्रण करणे तसेच संवेदनशील भागावर नियंत्रण ठेवणे इत्यादी बाबी परिणामकारकरित्या हाताळण्यासाठी अत्याधुनिक यंत्रणा म्हणून सीसीटीव्ही संनिरीक्षण यंत्रणा बसविण्याबाबतची कार्यवाही अनेक शहरांमध्ये/गावांमध्ये केली जात आहे. सीसीटीव्ही संनिरीक्षण यंत्रणा बसविण्यासाठी जिल्हा वार्षिक योजना, आमदार फंड तसेच स्थानिक स्वराज संस्थांच्या माध्यमातून निधी उपलब्ध करून दिला जात आहे. तथापि सीसीटीव्ही संनिरीक्षण यंत्रणा बसविण्याबाबत प्रकल्पाची गरज विचारात घेऊन सुसुत्रता येण्यासाठी तसेच प्रकल्प कार्यान्वित झाल्यानंतर दुरुस्ती व देखभालीची जबाबदारी निश्चित करणे आवश्यक असल्याने विविध शहरांमध्ये सीसीटीव्ही प्रकल्प राबविण्यासाठी मार्गदर्शक तत्वे संदर्भाधिन क्र.३ च्या शासन निर्णयान्वये निर्गमित करण्यात आली. सीसीटीव्ही प्रकल्पाच्या Model Detailed Project Report व Request For Proposal बाबत मार्गदर्शक तत्वे विहित करण्याची बाब तसेच संदर्भाधिन क्र.३ येथील दि.९.१.२०१७ च्या शासन निर्णयात सुधारणा करण्याची बाब शासनाच्या विचाराधीन होती. त्यानुषंगाने शासनाने खालीलप्रमाणे निर्णय घेतला आहे.

शासन निर्णय :

राज्यातील विविध शहरांमध्ये सुरक्षिततेच्या दृष्टीकोनातून सीसीटीव्ही संनिरीक्षण प्रकल्प राबविण्याबाबत खालीलप्रमाणे मार्गदर्शक तत्वे विहीत करण्यात येत आहेत.

(i) गृह विभागामार्फत निधी उपलब्ध करुन देण्याबाबतचे व गृह विभागामार्फत अंमलबजावणी होणारे सीसीटीव्ही प्रकल्प प्रस्ताव (Model Detail Project Report च्या आधारे) संबंधित पोलीस आयुक्त/पोलीस अधीक्षक यांनी तयार करुन तो पोलीस महासंचालक, महाराष्ट्र राज्य, मुंबई यांच्यामार्फत गृह विभागाच्या मान्यतेसाठी सादर करावा. सदर प्रस्तावामधील तांत्रिक बाबी तपासून त्यास माहिती व तंत्रज्ञान विभागाने मान्यता दिल्यानंतर प्रस्ताव उच्चस्तरीय शक्तीप्रदान समितीच्या मान्यतेसाठी सादर करण्यात येईल. सदर प्रस्तावास उच्चस्तरीय

शक्तीप्रदान समितीची मान्यता प्राप्त झाल्यानंतर प्रशासकीय मान्यतेचे आदेश निर्गमित्त करण्यात येतील. प्रशासकीय मान्यतेनंतर पोलीस महासंचालक यांनी Model Request For Proposal च्या आधारे Request For Proposal तयार करुन प्रस्ताव उच्चस्तरीय शक्ती प्रदत्त समितीच्या मान्यतेसाठी गृह विभागास सादर करावा. प्रस्तावास उच्चस्तरीय शक्ती प्रदत्त समितीने मान्यता दिल्यानंतर गृह विभागाकडून पोलीस महासंचालक यांना RFP प्रसिध्द करण्यासाठी कळविण्यात येईल. प्रकल्पाची अंमलबजावणी करण्याची कार्यवाही पोलीस महासंचालक कार्यालयाने प्रकल्प अंमलबजावणी समिती (Project Implementation Committee) गठीत करुन करावी. या प्रकल्प अंमलबजावणी समिती (PIC) मार्फत प्रकल्प संचालक याची निवड प्रक्रीया पार पाडल्यानंतर उच्चस्तरीय शक्ती प्रदत्त समितीमार्फत त्यास मान्यता देण्यात येईल. तद्नंतर पोलीस महासंचालक कार्यालय त्यांचे सोबत करारनामा (Service Level Agreement) करेल. प्रकल्प अंमलबजावणी समिती (PIC) मार्फत प्रकल्पाची अंमलबजावणी करण्याची कार्यवाही करण्यात येईल. तद्नंतर सीसीटीव्ही सनिरीक्षण प्रकल्पास निधी वितरणाची कार्यवाही करारनाम्यानुसार करण्यात येईल.

(ii) जिल्हा वार्षिक योजना (सर्वसाधारण) याखाली (District Planning Development Council) उपलब्ध निधी मधून सीसीटीव्ही प्रकल्पास निधी उपलब्ध करुन देण्याबाबतचे प्रस्ताव Model Detail Project Report च्या आधारे तयार करताना उपलब्ध निधी विचारात घेऊन संबंधित घटकाने संबंधित पोलीस आयुक्त/पोलीस अधीक्षक यांच्याशी विचारविनीमय करुन सविस्तर प्रकल्प अहवाल (Detail Project Report) तयार करावा व गृह विभागास सादर करावा. तद्नंतर माहिती व तंत्रज्ञान विभाग आणि गृह विभाग यांची मान्यता मिळाल्यानंतर शहरात सीसीटीव्ही संनिरीक्षण प्रकल्प राबविण्याबाबतची पुढील कार्यवाही संबंधित घटकाने / शहराने त्यांच्या स्तरावर करावी.

२. सीसीटीव्ही संनिरीक्षण प्रकल्प यशस्वीरित्या राबविण्यासाठी खालीलप्रमाणे स्थानिक सीसीटीव्ही संनिरीक्षण प्रकल्प समिती संबंधित प्रकल्पासाठी गठीत करण्यात यावी.

अ.क्र.	अधिकाऱ्याचे पदनाम	समितीवरील पद
१	पोलीस आयुक्त / पोलीस अधिक्षक	अध्यक्ष
२	जिल्हाधिकारी यांचा प्रतिनिधी	सदस्य
३	महानगरपालिका आयुक्त / स्थानिक स्वराज्य संस्थेचा प्रमुख	सदस्य
४	वाहतूक पोलीस प्रमुख	सदस्य
५	निवासी उपजिल्हाधिकारी	सदस्य
६	पोलीस आयुक्त /पोलीस अधिक्षक यांनी नामनिर्देशित केलेला अधिकारी	सदस्य सचिव

या समितीवर सीसीटीव्ही संनिरीक्षण प्रकल्प तयार करण्यासाठी सोबत जोडलेल्या परिशिष्ट क्र.१ मध्ये नमूद **Model Detail Project Report** मार्गदर्शक तत्त्वांनुसार प्रस्ताव तयार करण्याची कार्यवाही संबंधित घटकाकडून करण्यात यावी.

सदर शासन निर्णय महाराष्ट्र शासनाच्या **www.maharashtra.gov.in** या संकेतस्थळावर उपलब्ध करण्यात आला असून त्याचा संकेतांक २०२४०१२५१७४१२७२१२९ असा आहे. हा शासन निर्णय डिजीटल स्वाक्षरीने साक्षांकित करुन काढण्यात येत आहे.

महाराष्ट्राचे राज्यपाल यांच्या आदेशानुसार व नावाने.

RUPALI SANJOG KABARE

Digitally signed by RUPALI SANJOG KABARE
DN: c=IN, o=GOVERNMENT OF MAHARASHTRA, ou=HOME DEPARTMENT, 2.5.4.20=825ec39543f0d33deccec30f6ca54b1adc430443efec55f07e98dc173423779d, postalCode=400032, st=Maharashtra, serialNumber=5CB43A03D973FF96AABBF02A74864A4681399FE663D8FBDE0441A596BEB3ACDD, cn=RUPALI SANJOG KABARE
Date: 2024.01.25 17:49:50 +05'30'

(रुपाली कबरे)
कार्यासन अधिकारी, गृह विभाग

प्रत :
१. मा. मुख्यमंत्री यांचे प्रधान सचिव
२. मा. मंत्री (वित्त व नियोजन) यांचे खाजगी सचिव
३. मुख्य सचिव, महाराष्ट्र राज्य, मंत्रालय, मुंबई
४. अपर मुख्य सचिव, माहिती व तंत्रज्ञान विभाग, मंत्रालय, मुंबई
५. अपर मुख्य सचिव / प्रधान सचिव / सचिव, सर्व मंत्रालयीन विभाग
६. पोलीस महासंचालक, महाराष्ट्र राज्य, मुंबई
७. सर्व पोलीस आयुक्त
८. सर्व पोलीस अधीक्षक
९. महालेखापाल (लेखा व अनुज्ञेयता/लेखापरीक्षा), महाराष्ट्र १/२, मुंबई/नागपूर
१०. निवासी लेखा परीक्षा अधिकारी, मुंबई
११. सर्व जिल्हा नियोजन अधिकारी
१२. निवडनस्ती, पोल-३.

Guidelines for Installation of CCTV Surveillance System

Annexure - **1**

1) Funding

- Estimation and Fund Allocation to be done for the Capital Expenditure (Nonrecurring) as well as for at least 5 years of Operational Expenditure (Recurring). The funds required for the CCTV project can be explored from different sources like DPDC, MLA/MP fund, funds from Municipal Corporation, etc.
- There is a tendency to treat such projects as Capital Expenditure Projects which is not true since Operational Expenditure in CCTV projects is quite substantial and needs to be provisioned carefully while planning the project.
- It is recommended not to make down payment to the vendors beyond 50%of the total project cost (Capital + Operational Costs) at successful Go Live stage. Remaining payment could be in 20 equal installments on quarterly basis, after adjusting for penalties as per the Service Level Agreement (SLA).
- Ownership of the project shall be transferred to the City Police Commissionerate / District SP Office. To facilitate this, the concerned heads of the units shall establish a system to ensure the continued operation of the project after 5 years.

2) Camera Sites, Types, Connectivity

i. Selection of sites to be done by CP (Commissioner of Police)/ SP (Superintendent of Police) after considering the requirements of Police, Traffic Department and Municipal Corporation / Local Body / Zilla Parishad.

ii. Public places with high footfall, major traffic junctions, hot spots of crime, places with religions importance, routes of religious processions, Vital Installations (like flyovers, bridges, electricity plants, distribution points, dams, water supply and pumping stations, water filtration plants, statues of eminent personalities etc.) and entry & exit points to the city should be given priority. Approach roads to important government buildings should also be covered.

iii. Bus Depots, Railway stations, Airports, Malls, Hospitals, Hotels, etc. may have their own systems, and their integration to the planned system must be considered.

iv. Care should be taken while finalizing the number and types of CCTV cameras at each selected location. This should be decided by the concerned Committee (स्थानिक संनियंत्रण समिती) and based on the requirements.

v. Normally 75% of the total cameras should be Fix Box Cameras (Including ANPR) and the

rest can be PTZ (Pan, Tilt, Zoom) cameras. The number of PTZ cameras should not be more than 30% of the total number of cameras. The number of PTZ cameras should be determined keeping in view the availability of staff and need for constant viewing. However, each location has different requirement, and there cannot be any fixed ratio. This should be finalized after a detailed survey by the authorities concerned for each location.

vi. Option of Solar panel usage may be explored in the suitable locations.

Video Management System (VMS) and Control:

i) The Video Management System (VMS) must be readily accessible on desktop computers as well as on portable electronic devices (PEDs) such as mobile applications. Access to the VMS via the mobile application should be restricted solely to authorized personnel in accordance with our CCTV policy.

ii) Remote access to the Video Management System (VMS) necessitates the implementation of dual-factor authentication. Furthermore, it is imperative that all data within the desktop VMS System remains encrypted during transit and while at rest. This encryption should adhere to the standards of secure Socket Layer (SSL) and Transport Layer Security (TLS) certifications, in strict accordance with industry-established best practices.

iii) VMS Functionality: The Video Management System (VMS) provides the capability for simultaneous viewing of multiple camera feeds on designated workstations.

iv) PTZ Control: To manage PTZ cameras effectively, every viewing-cum-controlling station should be outfitted with a joystick controller. Only authorized personnel are permitted to operate PTZ movements.

ANPR and Video Analytics:

i) CCTV Committee Evaluation: Prior to their incorporation into the project scope, the inclusion of ANPR (Automatic Number Plate Recognition), thermal, sound cameras and other IOT based analytics, video analytics, alert systems, etc. demands thorough evaluation by the CCTV Committee.

ii) ANPR Implementation Recommendation: ANPR functionality is recommended for cameras positioned in areas where vehicles adhere to lane restrictions and operate at low speeds. Toll Naka's present suitable conditions for the implementation of ANPR technology. Furthermore, to enhance city security and traffic monitoring comprehensively, it is also advisable to install Automatic Number Plate Recognition (ANPR) cameras at all entry and exit points of the city. This dual implementation will facilitate vehicle tracking for both entry and exit purposes while effectively managing the traffic flow.

iii) Ensuring **Illumination:** To ensure optimal video quality during evenings and nights, it is essential for local authorities to prioritize adequate lighting at designated locations in accordance with Section 249 of the Maharashtra Municipal Corporations Act (1949).

Depending on specific needs, the use of Infrared Illuminators is recommended to enhance surveillance capabilities.

iv) The video feeds data from all aggregation points should go to Centralized Data Centre or Server Room for recording, from where the data can be viewed live at the control command center and police stations.

v) Standardized Signs informing the public of the existence of CCTV cameras may be placed at suitable locations.

3) Guidelines for Infrastructure components

i) End-of-Life products to be avoided. It is thus important that the OEMs (Original Equipment Manufacturer) are asked to undertake that they would be supporting the equipment for the project life cycle.

ii) Critical / Core components of the system should not have any requirements of proprietary platforms and should conform to open standards. This shall eliminate the risk of vendor-locking. All Servers/Blade servers, Active Networking Components, Security Equipment and Storage Systems proposed should be from well-known OEMs (like those who are listed as top 5 as per Gartner / IDC reports).

iii) All the Cameras and Video Management Software (VMS) of the project should be from OEMs who are amongst Top 10 Vendors for Market Share in terms of Revenue as per the latest (on the date of bid submission) published IMS report.

iv) A helpdesk and facility management services (FMS) desk should be set up at central location. This facility would be manned by the FMS staff of the System Integrator. All calls relating to camera malfunctioning, network failure, downtime of the system should be attended promptly (as per the specified Service Level Agreements) by the System Integrator.

v) As far as possible, Disaster Recovery (DR) site should be planned for the Data Center.

vi) It would be a good idea to subject all the modules of the software involved in project to

a) Since Security Audit are mainly needed for Publicity hosted Websites. This Project might require “Third Party Audit” which is detailed in other section of this Policy.

b) All software licenses should be in the name of the Chairman of the CCTV Surveillance Project Committee (e.g., Commissioner / Superintendent of Police of the respective City / District).

4) Storage Guidelines

i) Video data should be stored securely in centralized location. It should be treated as a classified document. All video data from all cameras should be stored without any human intervention, either prior to viewing or while viewing.

ii) Primary Storage (to make data available readily for the system users) should be designed to store data **for 30 days**, while Secondary Storage should be designed to store data for **30 – 180 days.**

iii) If the system envisages use of ANPR system, such data should be stored at least for **180 days** on secondary storage or as per latest Legal Guidelines in this regard.

iv) Data on Primary & Secondary Storage would be over-written automatically by newer data after the stipulated period. If some data is flagged by the authorized personnel or sought by way of court orders, there should be provision to store it for longer duration. CCTV Committee should meet every 3 months to take such decisions for preservation of the flagged data beyond 90 days on secondary storage.

v) Copies of the Video footage with evidentiary value should be prepared with watermarks and date-timestamps, using the VMS, and kept in the proper custody of Police Department. Member Secretary of the CCTV Committee, or his nominee, should ensure the chain of custody and integrity of the footage.

vi) USB ports / USB Drives / External Drives/ CD-DVD Writers on all user desktops at the viewing stations should be disabled. Such devices pose threat of infection from viruses, Trojans, Malwares, etc. as well as threat to security of project data.

vii) Since there would be cases where-in Police Department / concerned, authority may have to produce the CD / DVD of the video feed as evidence in court of law. It is necessary that creating such evidence on CD / DVD / any other storage media is done as per the legal requirements so that the evidence is considered as un-tampered in the court of law.

5) Viewing of the Camera Feeds

i) Frame Rate Selection: It is strongly advised that the CCTV system operates with a frame rate of 15-20 Frames per second (FPS) for both viewing and storage purposes. In case there is no movement in front of the camera, video can be viewed and stored 8 FPS.

ii) In scenarios where bandwidth constraints are not limiting factor, the option to view video feeds at a higher FPS is available. Nevertheless, it is crucial to emphasize that storage should not exceed the 25 FPS threshold. This measure is in place to effectively manage and control the associated storage costs.

iii) It is important that the bandwidth estimation is done properly for different types of cameras (considering the proposed resolution and FPS) by the vendors. Bidders should be asked to state the minimum bandwidth provisioning carried out by them and demonstrate that the required quality is managed within the same bandwidth.

iv) **Camera Specification Caution:** During the specification and procurement of CCTV cameras, meticulous care must be exercised. Particular attention should be devoted to ensuring that camera specifications are chosen in a manner that guarantees optimal video quality and performance.

v) There should be at least one Control Room in the city where all the feeds can be viewed. It is

recommended that provision be made to simultaneously view any 10% of the total cameras in such control room.

vi) Police Stations may be equipped to view cameras of their jurisdiction. Provision may be kept to simultaneously view feeds of any 50% of camera feeds under their jurisdiction. "Based on criticality of the Police station and sensitivity of the area this % can be increased.

vii) Camera Feed Viewing Center may be setup at Municipal Corporation / Local Body / Zilla Parishad offices for monitoring the video feeds of vital installations & important locations for ensuring better emergency response.

viii) Camera Feed viewing center should also be set up at Traffic Control Room (if it exists) for efficient traffic management. The ratio of PTZ Camera suggested in earlier section of this policy may be modified / increased if the surveillance requirement is for mostly Traffic Management and / or involves long stretches of Roads.

6) Collaborative Monitoring by Public and Private Establishments

i) All video feeds from various ICCC (Integrated Command and Control Centre) Centers across different locations shall be seamlessly integrated into a centralized hub, either at the CM War Room or the State Level Control Room. This integration is essential to provide real-time monitoring and response capabilities in various scenarios, including but not limited to disasters, crimes, and riots.

ii) Apart from the CCTV network being installed by the CCTV Committee, there are several establishments like hotels, malls, theatres, office buildings, residential societies, hospitals, schools, colleges, railway stations, bus stations, etc., where CCTV cameras may exist. The CCTV committee should ensure that such private/public establishments are properly guided regarding the following:

- The quantity, type, and placement of CCTV cameras in that establishment.
- Technology Standard to be followed by the establishments to allow compatibility of data / systems with the City Surveillance System.
- Video Storage Guidelines.

iii) To ensure that private/public establishments are properly guided, CCTV committee should repeatedly and adequately publicize to these establishments, that the committee can provide guidance with respect the CCTV installations and above-mentioned parameters.

iv) The integration of location feeds into a centralized control room, along with the provision of a backup facility, aims to enhance the efficiency and effectiveness of the CCTV surveillance policy during critical situations. This setup will aid law enforcement and emergency response agencies in swiftly addressing incidents and ensuring public safety.

v) The CCTV committee should adopt and enforce Standard Operating Procedures (SOPs) for collection of video data from such establishments in case of an incident.

vi) State Home department is engaging with various stakeholders to issue a set of guidelines (Called Guidelines for Collaborative CCTV monitoring) to connect the Private / Public establishment CCTV Systems with the City Surveillance System, with help of dedicated networking connectivity (including converters for analog systems) in an event of any security breach or any untoward incident. CCTV Committee should adopt and enforce such guidelines issued from Home Department from time to time.

vii) The CCTV system that is being setup should have a provision to provide link to the "State Level Control Room" once it is setup.

7. Service Level Agreement for CCTV Camera System Maintenance

To address non-working CCTV cameras or their components within a defined timeframe and to ensure the efficient operation of the surveillance system while optimizing maintenance costs through the implementation of a Service Level Agreement (SLA).

i) **Service Level Agreement (SLA)**:

An SLA will be created in collaboration with the system implementer to govern the maintenance of the CCTV camera system.

The SLA will clearly outline the specific terms, conditions, and expectations regarding the resolution of non-working cameras or components.

ii) **Definition of Non-Working Components**:

Non-working components encompass any malfunctioning CCTV cameras or related parts that impede the proper functioning of the surveillance system.

iii) **Resolution Timeframe**:

Once non-working components are identified, the implementer is obligated to resolve the issue within a predefined timeframe.

The resolution timeframe will be mutually agreed upon in the SLA and should be reasonable, considering the criticality of the camera's location and function.

iv) **Monitoring and Reporting**:

Routine monitoring of the CCTV camera system's performance will be conducted to identify non-working components.

Any non-working components discovered during monitoring must be promptly reported to the implementer for resolution. Detailed records of these issues and their resolution status will be maintained.

v) **Cost Reduction Mechanism**:

If the implementer fails to meet the agreed-upon resolution timeframe for non-working components, a cost-reduction mechanism will be activated.

The reduction in charges will be calculated based on the duration of non-resolution, with the deducted amount subtracted from the maintenance fees payable to the implementer.

vi) **Review and Modification**:

The SLA will undergo periodic reviews to assess its effectiveness and relevance.

If necessary, modifications to the SLA may be made to accommodate changing circumstances or requirements.

vii) **Compliance**:

All relevant stakeholders, including the implementer and those responsible for monitoring, are expected to adhere to the terms outlined in the SLA.

Failure to comply with the SLA may lead to penalties or contract termination, as specified in the agreement.

viii) **Maintenance**:

The total contract period for the System Integrator should include 5 years of Operational & Maintenance period, after successful Go Live.

8. **Other Recommendations**:

i) In case the CCTV committee feels the need of a consultancy firm for preparation of Detailed Project Report (DPR), RFP/Tender document, Assistance in Tender process, Project Management (till its implementation and Go Live stage), it may seek consultancy services of consulting firms empaneled by DIT/Government of Maharashtra for Governance projects.

ii) It is recommended minimum requirements of the technical staff for Data Center Support & End User Hardware support is defined upfront.

iii) Necessary power backup needs to be ensured for Data Centers & Control Centers through Online UPS for 30 minutes. (To ensure it is a cost effective solution) and automatic DG sets to ensure that power is available to the Data Center & Control Rooms on 24 x 7 x 365 basis. Necessary power backup would also be required for cameras through UPS. CCTV Committee shall also work with local utility providers to ensure that the power outages to camera locations are avoided / minimized.

iv) It is important that the contract clearly identifies the breach conditions for the System Integrator and the Exit Policy.

v) CCTV Committee would approve the RFP. It is recommended that bids be called in 2 envelope system (Technical Envelope & Commercial Envelope). RFP should specify 70% as the passing marks in Technical Evaluation to open Commercial Bids, and thereafter the bidder should be selected on L1 basis.

vi) Technical evaluation of bids may be carried out broadly on various parameters viz. financial strength of the bidder, experience of the bidder, quality of people proposed, technical

features of the proposed solution, proposed methodology, understanding of the bidder of the project requirement, etc. Percentage of marks to be given for each category should be decided and mentioned in the RFP by CCTV committee as per the project requirement.

vii) It is important that certain items needed for future expansion (such cameras, bandwidth for each additional cameras, poles, networking equipment such as routers/switches etc.) be identified as Additional Items, which should be included in calculation (by way of adding certain quantities in commercial calculation). However, these additional items shall no form part of the initial work order, but the prices offered by bidder must be used for future expansion orders.

viii) Urban Local Bodies shall consider waving off RI / RO charges for the aforesaid CCTV Installation Projects.

9. Third-Party Audit in CCTV Video Surveillance Policy:

To ensure the robustness and effectiveness of our CCTV video surveillance system, an annual third-party audit shall be performed. This audit will be entrusted to a certified audit firm to maintain objectivity and uphold the highest standards of security and privacy. The primary objective of this audit is to evaluate the overall performance, compliance with relevant regulations, and the protection of data and privacy within our surveillance system.

The third-party audit will encompass a comprehensive assessment of the following key aspects:

a. **System Integrity:** The audit will scrutinize the operational integrity of the CCTV video surveillance system, checking for any vulnerabilities or weaknesses that may compromise its functionality.

b. **Compliance:** It will verify compliance with local, national, and international regulations pertaining to video surveillance, data retention, and privacy, ensuring that our system adheres to all necessary legal requirements.

c. **Data Security:** The audit will examine the measures in place to protect the recorded data from unauthorized access or tampering. This includes access controls, encryption, and data storage protocols.

d. **Privacy Safeguards:** Assessments will be made to confirm that the surveillance system respects individuals' privacy rights and adheres to our established privacy policies and procedures.

e. **Camera Functionality:** The functionality and positioning of cameras will be reviewed to ensure that they effectively cover the designated areas without infringing upon private spaces.

f. **Recording and Storage:** The audit will verify that the recording and storage processes are in compliance with data protection laws, and that recorded data is retained for an appropriate duration.

g. **Incident Response:** The assessment will include a review of the system's incident response procedures, ensuring that any security breaches or incidents are promptly identified and addressed.

h. **Access Control:** The audit will assess the management of access to live feeds and recorded data, verifying that only authorized personnel can access the system.

The third-party audit report shall be submitted to the CCTV Committee upon completion. Any identified deficiencies or areas requiring improvement will be addressed promptly to enhance the security and effectiveness of our CCTV video surveillance system.

10. GIS Mapping

To enhance the effectiveness and management of our CCTV Surveillance system, it is imperative to integrate Geographic Information System (GIS) mapping. This integration will provide a comprehensive overview of our surveillance infrastructure, ensuring a more proactive and efficient security approach.

The GIS mapping component will encompass the following essential elements:

a. **Location Data**: Each CCTV camera's precise geographical coordinates, including latitude and longitude, will be recorded in the GIS system. This information will enable real-time tracking of camera locations, aiding in incident response and maintenance.

b. **Status Monitoring**: The GIS mapping will continuously monitor and update the status of each CCTV camera. This includes distinguishing between functioning and non-functioning cameras. Timely identification of non-operational cameras will be crucial in maintaining an uninterrupted surveillance network.

11. E-tendering Protocols

The department should adhere to a comprehensive E-Tendering protocol, which includes the following essential steps and documents:

a. Initiation: Begin with a Notice Inviting Tender to inform potential bidders.
b. Quantities: Specify the approximate quantities of required items.
c. Communication: Send out a Letter to the Prospective Bidders to provide necessary information.
d. Checklist: Utilize a structured checklist to ensure all essential elements are covered.
e. Contract Terms: Define the General Terms & Conditions of Contract for clarity.
f. Technical Aspects: Include a Technical Bid Performa for technical specifications.
g. Itemization: Provide an unpriced bill of Quantities (BOQ) for item details.
h. Financial Aspects: Include the Financial Bid section for pricing information.
i. Integrity Assurance: Incorporate a Pre-Contract Integrity Pact for ethical commitment.
j. Acceptance: Issue a Tender Acceptance Letter to the successful bidder.
k. Authorization: Grant authorization for attending the Bid Opening event.
l. Equipment Distribution: Specify the distribution plan for CCTV cameras by location.
m. Technical Requirements: Outline Technical Specifications for the equipment.
n. Security Assurance: Include a Bank Guarantee Form for Performance Security.

12. SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

1. Access to the physical location where the CCTV footage is digitally stored during the retention period is limited to designated personnel, authorized invited guests, and external stakeholders. Physical security protections include: guards, access logs, and locked facilities requiring badges or access cards for entry. All external stakeholders must be screened and authorized by the staff designated.
2. The ability to review CCTV video in real-time is confidential-password-protected and access is restricted to only authorized users. Personnel authorized to view live CCTV system video consist only of designated personnel in various commands, whose access has been requested by their Commanding Officer, and approved by Unit In charge. The personnel CCTV system access is adjusted or removed when the access is no longer necessary for concerned personnel to fulfill their duties (e.g., when personnel are transferred to a command).
3. Personnel must abide by security terms and conditions associated with computer and case management systems of the CCC, including those governing user passwords and logon procedures. CCC personnel must maintain confidentiality of information accessed, created, received, disclosed, or otherwise maintained during duty and may only disclose information to others, including other members of the CCC, only as required in the execution of lawful duty.
4. Personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to confidentiality policies may subject CCC (Command and Control center) personnel to disciplinary and/or criminal action. CCC personnel must confirm the identity and affiliation of individuals requesting information from the CCC and determine that the release of information is lawful prior to disclosure.

Annexure - **2**

Scope of Work for Surveillance Project

Considering the overall project requirements, the scope of work for the bidder can be classified into five main components as follows:

Component # 1 Surveillance Equipment

Component # 2 Network Connectivity

Component # 3 Data Centre (Servers, Storage, Application etc.)

Component # 4 Command/Viewing Centers

Component # 5 Helpdesk and FMS (Facility Management Service)

It is important that the RFP (Request for Proposal) defines scope quantitatively and qualitatively for each of the above scope elements. Large part of the qualitative part of the scope should be covered through the benchmark specifications.

It is important that the System Integrator's scope of work clearly defines following activities:

Pre-Implementation / Implementation Services

1) Finalize the Camera distribution and exact positions of the Cameras at different locations in consultation with Police Department
2) Obtain all necessary legal / statutory clearances & Erect Poles
3) Provision of the Electricity at Camera Locations, at Command Centers
4) Submit the design of network connectivity as part of proposal & then carry out the connectivity implementation in a planned manner
5) LAN connectivity requirements at locations
6) Supply, install, commission & configure cameras
7) Design & Implementation of the Data Center (s)
8) Preparation of Detailed FRS, SRS and SDD for the customized Video Surveillance System
9) Integration of Camera Locations on the GIS Map of the city (if available)
10) Unit Testing of the Cameras / Connectivity / Data Center Equipment
11) Composite Testing of the overall system
12) Preparation and implementation of the Information security policy and Backup policy.
13) Training and Capacity Building for the Police Department for operationalization of the system. Training should involve both Functional & Administrative Trainings. Submission of System Documents, User Documents, etc.

Post Implementation Services (for the period of 5 years post Go Live)

i. Helpdesk and Facilities Management Services.
ii. Refresher Training
iii. Patch Updations, Version Upgradations of the System
iv. Support to police department for sending the video data to other cities / to accept video data from other cities for investigation purpose
v. Co-ordination with Picture Intelligence Unit (PIU) of Mumbai Surveillance Project
vi. Addition of Cameras, other components for scaling up of the project (it is required that unit prices for such components are captured at the tendering stage itself)
vii. Hand-over of the system at the end of contractual period along with handholding support to train and run the system efficiently and all documentation required to operate and maintain the system.

Annexure - **3**

Suggestive Qualifying Criteria for vendors

i. The bidder must be a registered corporate in India, registered under the Companies Act 1956, or a Govt. Organization. The bidder should be operating in India for the last three years as on the date of submission of bid.

ii. The bidder should have positive net worth as on current audited financial year

iii. The bidder should have an overall turnover (gross revenue) of at least **<50%of total estimated project cost – Capital Cost + Operational Cost for 5 years> from** IT/ITES/Telecom during each of the last 3 financial years as on the date of submission of bid.

iv. In case of consortium, the consortium partners should have overall turnover (gross income) of at least <**20% of total estimated project cost – Capital Cost + Operational Cost for 5 years>** from IT/ITES/Telecom during each of the last 3 financial years as on the date of submission of bid.

v. The bidder should have experience of at least one project of installation of turn-key CCTV based surveillance system including implementation of Video Management System. Such project should have at least 50 cameras providing video feeds. Such project must also be operational (with more than 90% camera working) on the day of submission of the bid and during technical evaluation period.

vi. The bidder should have an ISO 9001:2008 certification or should be an SEI CMM Level 3 or above certified organization.

vii. Bidder should not have been debarred / black-listed by Central / State Government in India, at the time of submission of the RFP.

In case of consortium, a consortium partner to be allowed to participate in one consortium bid unless the partner is an OEM or Network Service Provider or Data Center Provider and can be part of consortium only as OEM or Network Service Provider or Data Center Provider respectively.

*****

Annexture-IV

Model Request for Proposal

for

CCTV based SurveillanceSystem For <Location>

Issued By

DIT, Government of Maharashtra

Confidential

Table of contents

Contents

1. [Confidentiality]

This document has been circulated for limited circulation only, amongst the vendors who have requested for the purchase of RFP for the Design, Development, Implementation & Maintenance of CCTV based Surveillance System for< >city. Information shared to the bidders through this document is confidential in nature and pertains to security of City. Any further circulation of this information, without prior permission of the Department, Government of Maharashtra, is prohibited and would attract punishment / penalties.

2. Glossary & Definition

Terms	***Meaning***
AMC	Annual Maintenance Contract
AP	Access Points
ATS	Annual Technical Support
BOM	Bill of Material
CEO	Chief Executive Officer
DC	Data Center
DD	Demand Draft
DR	Disaster Recovery
EMD	Earnest Money Deposit
FRS	Functional Requirement Specifications
GIS	Geographical Information System
GPS	Global Position System
ICCC	Integrated Command Control Center
ICT	Information and Communication Technology
INR	Indian Rupee
LoI	Letter of Intent
MTTR	Mean Time to Repair
OEM	Original Equipment Manufacture
O&M	Operations and Maintenance
PBG	Performance Bank Guarantee
POE	Power over Ethernet
PQ	Pre-Qualification
RFP	Request for Proposal
RO	Request Order
SAN	Storage Area Network
SI	Bidder
SLA	Service Level Agreement
SOP	Standard Operating Procedures
SRS	Software Requirement Specifications

SCADL	Smart City Ahmedabad Development Limited
TQ	Technical Qualification
UAT	User Acceptance Testing
GPRS	Global Packet Radio Service
GSM	Global System for Mobile Communication
BoQ	Bill of Quantity
COTS	Commercial-off-the-shelf
Model RFP	Model RFP of Government of India and Government of Maharashtra to be taken into consideration during preparation of the CCTV RFP for <Location>

3. Scope of Work for the Systems Integrator- O&M

Implementation & Maintenance

The selected Systems Integrator should have the overall responsibility to design, build, implementation, operate, and maintain the <Location> surveillance project for a period of Min five years from the date of successful completion of Acceptance Tests/Go Live

Listing of broad components of the scope of work of the Systems Integrator is given below for quick reference:

1	**Cameras**	• Type & Unit ---------- PTZ Cameras • Type & Unit ----------Thermal Cameras • Type & Unit ---------- Fixed Box Cameras • Type & Unit ----------ANPR Cameras with ANPR System • Type & Unit ---------- Dome Cameras • Type & Unit ----------Multilense Cameras • Analytics support for ---------- Type & Unit of Camera • Location and unit of cameras as per dept.
2	**Network**	• Between • Cameras & Aggregation Points • Aggregation Points & Data Centers/Server Room • Data Centers/Server Room and DR • Data Centers/ Server Room & Integrated Command Centers • Data Centers/Server Room & the respective Viewing Centers (Regional Offices, Zonal Offices, Police Stations, other Govt office & HQ) • Data Centers/Server Room & Mobile Vans • Private / public establishments & DataCenters/server room
3	**Data Centers/Server Farm/servers/ cloud**	• Data Centers and DR separated by 100 km in Active - Active Mode, can be on Sharing Mode with other government CCTV Datacenter/Server room/cloud as secondary option • Each Data Center/Server capable to handle 100% of load, but catering to 50% load in normal circumstances.

4	**Application& Software's**	1. Video Management System 2. Analytics Software for Picture Intelligence Unit like Facial Recognition System using AI/ML (need based) 3. Application for Enterprise Management (Network, Help Desk,SLA Mgmt.) 4. Application for Vehicle Tracking System(optional) 5. RDBMS 6. Customized Dashboard for Surveillance at different levels
5	**Command / Viewing Centers (ICCC & feed center)**	1. For EVERY CITY 1 ICCC 2. Command Control Centre at CP Office /SP office 3. Viewing of Feeds at ---------- Police Stations, ---------- Regional /Divisional Offices &---------/state level----need basis
6	**Picture IntelligenceUnit**	• Software enabled and on need basis • Oversee the Implementation of ANPR System & Other Analytics Systems
7	**Collaborative Monitoring**	• Incidence based access to the Surveillance System setup by private / public institutions (----------)
8	**Helpdesk & FMS**	• Provision of 24 / 7 Help Desk System for technical / operational support & Maintenance of the IT / Non-IT Infrastructure

The detail work to be undertaken by the successful bidder for setting up & operationalization of the city surveillance project is given in subsequent sections and is to be performed as per the specifications and conditions mentioned in this RFP and as per any further amendments issued and the contract to be signed with the successful bidder subsequently. From the perspective of project implementation, the scope has been categorized as follows:

A) Implementation Services

- Assess and Prepare- in collaboration with user dept
- User capability development-Functional requirement
- Implementation

B) Post-Implementation Services

- Maintain

The subsequent sections are divided as follows to give the overall scope & the broad list of the deliverables:

Implementation Services

- Finalization and submission of a detailed technical architecture and submission of a detailed project plan
- Implementation of Component #1: Surveillance Equipment
- Implementation of Component #2: Network
- Implementation of Component #3: Data Centers/server room
- Implementation of Component #4: Application Portfolio

- Implementation of Component #5: Command Centers
- Implementation of Component #6: Picture Intelligence Unit
- Preparation and implementation of the Surveillance system information security Policy, including Policies on backup
- Training to the identified Police Personnel for operation of the system and further Capacity Building
- Final Acceptance Testing of project components
- Planning, Suggesting and Submitting the Surveillance System up-grade plan(s) for five years from the date of acceptance along with detailed specifications including drawings, which should be in-line with the vision of the project
- System Document, User Document as per ITIL (Information Technology Infrastructure Library) standards

Post-Implementation Services

- Component #8: Services towards Collaborative Monitoring
- Component #9: Help Desk and Facility Management Services
- Planning, Suggesting and Submitting the Surveillance System up-grade plan(s) for five years from the date of acceptance along with detailed specifications
- Hand- over of the system at the end of contractual period along with all documents required to operate and maintain the system.

1.1 Finalization and submission of a detailed technical architecture

Submission of a detailed project plan & Implementation timelines - Post work order acceptance, the Systems Integrator needs to deploy the team proposed for the project and ensure that a Project Inception Report is submitted to GoM, which should cover following aspects:

- Detail of the Project Team members, their roles & responsibilities
- Approach & methodology to be adopted to implementation the Project (which should be in line with what has been promised during bidding stage but may have value additions / learning in the interest of the project).
- Responsibility matrix for all stakeholders
- Risks the bidder anticipates and the plans they have towards their mitigation.
- **Detailed Project implementation Plan**, specifying dependencies between various project activities /sub-activities and their timelines.

#	Activity	Timeline
1.	Bid Process Management	T + 1 Month
2.	Contract Signing with the winning bidder	T + 2 Months
3.	Prepare SRS, SDD for the Entire Video Surveillance System	T + 3 Months
4.	Supply, Installation, Configuration of various equipment's, components, systems at Data Center	T + 4 Months
5.	Installation of Cameras at <Area 1> <Area 2> <Area 3> .. **(Phase I) & Operationalization of the System on Pilot basis**	T + 4 Months

6.	Training and Capacity Building for the Police Personnel	T + 4 Months
7.	Installation of Cameras at other locations (If necessary)	T + 5 Months
8.	Final Acceptance Testing (FAT) for Video Surveillance System, Data Center Equipment's & Phase I Cameras	T + 5 Months
9.	**Go Live for rest of the Locations**	T + 6 Months
10.	Preparation and Submission of the following Manuals a. Systems Administration Manuals b. User Manuals c. Installation Manuals d. Operational Manuals e. Maintenance Manuals	T + 6 Months
11.	Operations and Maintenance post Go-Live	5 Years

Thereafter, within 3 weeks, SI shall submit the detailed Technical Architecture which should take into consideration following guiding principles:

- **Scalability** - Important technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of city/ Location.
- **Availability** - Components of the architecture must provide redundancy and ensure that are no single point of failures in the key project components.
- **Security** - The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc.
- **Manageability** - Ease of configuration, ongoing health monitoring, and failure detection is vital to the goals of scalability, availability, and security and must be able to match the growth of the environment.
- **Interoperability -** The system should have capability to take feed from cameras installed by private / Govt. at public places, digitize (if required) & compress (if required) this feed & store as per requirements.
- **Open Standards** - System should use open standards and protocols to the extent possible.

1.2 Third Party Auditor (TPA).

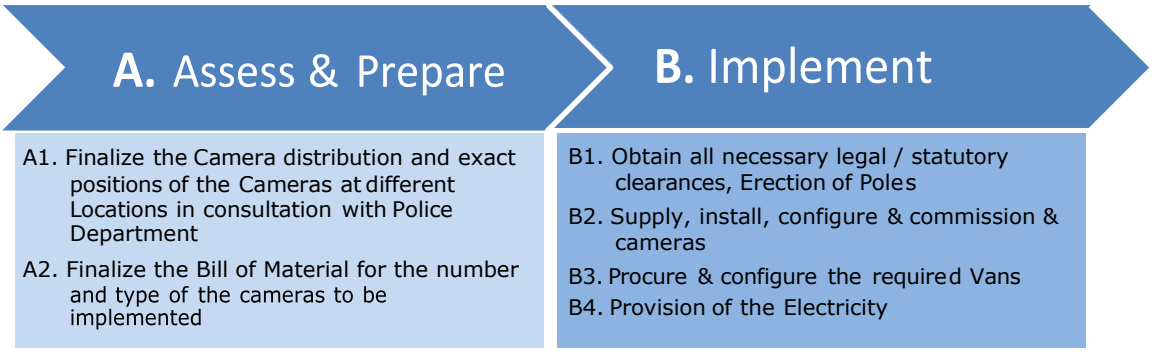
Department would carry out the Security Audit of the entire system in approx. 3 months of Acceptance / operationalization through a Third-Party Auditor (TPA). The following guidelines need to be observed for security

- Build a complete audit trail of all activities and operations using log reports, so that errors in system – intentional or otherwise – can be traced and corrected.
- The most appropriate level of security commensurate with the value to that function for which it is deployed must be chosen
- Access Controls must be provided to ensure that the system is not tampered or modified by the system operators.

- Implementation data security to allow for changes in technology and business needs.

1.3 Implementation of Component #1: Surveillance System

- This Component primarily would cover planning & implementation of the Cameras at different locations identified by Police department & on the mobile vans.



1.2.1 Assess & Prepare

A1. Finalize the Camera distribution and exact positions of the Cameras at different Locations in consultation with Police Department

- Bidders are required to note that while executing the project, the successful bidder shall prepare the final camera distribution plan at all the camera locations in discussion with Police & user Department.
- Actual place for placement of pole & number of cameras at each location, type of cameras, fixation of height & angle for the cameras would be done carefully to ensure optimum impact.
- Payments to be made to the Systems Integrator shall be based on actual number of cameras installed and unit rates quoted by the successful bidder shall be used to arrive at the same.

A2. Finalize the Bill of Material for the number and type of the cameras to be Implemented

As per the current plan of the user Department, about ------locations need to be covered through the surveillance cameras. Indicative list of these locations along with the Police Department's assessment of the camera requirements is given in of the RFP. SI shall prepare the detail report on Edge level requirements – Cameras (types & numbers), Camera Mounting requirements, Power Requirements, Connectivity Requirements. Indicative list of the Edge Level Hardware / Services is as follows:

- Cameras (Fixed Box Cameras, PTZ Cameras, Long Range Thermal Cameras)
- IR Illuminators, Managed Switches, Routers
- Junction boxes, Pole / Mast
- Digging & Trenching
- Networking cables and other related infrastructure
- Provisioning of Electric al Power

1.2.2 Implementation

B1. Obtain all necessary legal / statutory clearances & Erect Poles

Successful Bidder will have to identify and obtain necessary legal / statutory clearances for erecting the poles and installing cameras, for provisioning of the required power, etc. It is important to mention that a timely communication and required follow-up will be required by the successful bidder for the clearances. SI will have to then supply & erect poles at these locations well in advance to meet the camera installation timelines.

During post-implementation period, in case the Pole is damaged by a vehicular accident (or due to any other

reason outside the control of SI) and needs repair, then the corresponding cameras won't be part of the SLA monitoring for max. 15 days. That means, SI will need to repair / have the new pole within 15 days of the incidence. Post 15 days, the corresponding cameras would be again considered for SLAs. Damages are to be borne by SI in such cases through proper insurance.

B2. Supply, install, commission & configure cameras

The successful bidder will be required to supply, install, configure, and integrate the surveillance cameras at the identified locations and then undertake necessary work towards their commissioning. The successful bidder will also be commissioning the surveillance cameras required in the Mobile Vans. It is a must that the poles erected to house cameras are good, both qualitatively and aesthetically. Bidders are required to ensure that Cameras proposed are capable to meet these benchmark specifications and are also able to adhere to the functional requirements specified in Annexure 2. Benchmark specifications for various types of cameras to be supplied & operationalized as part of this project are given in Annexure 3.

SI should use the industry best practice while positioning and mounting the cameras. Some of the check- points which need to be adhered by the SI while installing / commissioning cameras are as follows:

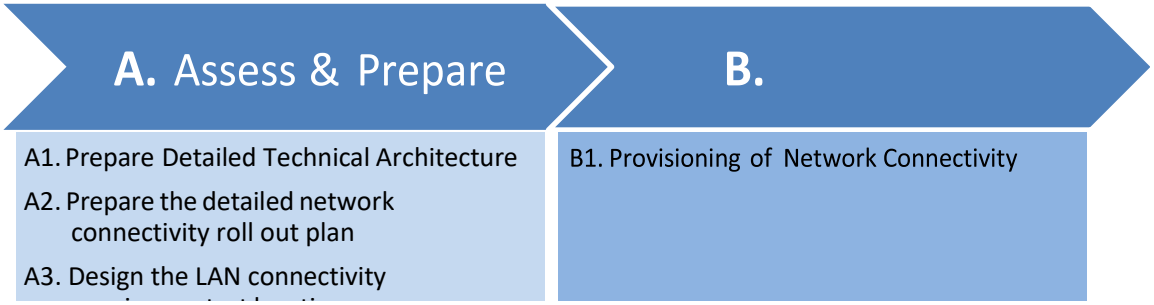
- Ensure Surveillance objective is met while positioning the camera, create the required field of view
- Ensure appropriate housing is provided to protect camera from the on-field challenges
- Carry out proper adjustments to have the best possible image
- Ensure that the pole / mast implementation is vibration resistant

B4. Provision of the Electricity

For the successful commissioning & operationalization of the cameras and to provide the video feeds to Command Centers and Police Stations, the successful bidder will be required to provide electricity to the cameras through the aggregation point. Since this component has dependency on approval from other agencies, it is recommended that SI plans this requirement well in advance & submits the application to the concerned electricity distribution agency. Registrations of Electrical connections are to be done in the name of SI. The SI to carry out study and identify locations to provide UPS backup, depending upon power situation across locations, to meet the camera uptime requirements.

Implementation of Component #2: Network Connectivity

Network Connectivity is one of the most important components of the project and needs very careful attention in assessment, planning and implementation. It is important not only to ensure that the required connectivity is provisioned within the required timelines but also ensure that it is reliable, secure and supports the required SLA parameters of Latency, Jitter, Packet Loss, and Performance.



1.3.1 Assess & Prepare

A1. Prepare the detailed network connectivity roll-out plan

The successful bidder shall prepare the overall network connectivity establishment plan for this project. The plan

shall comprise of deployment of network equipment's at the locations to be connected over network, any clearances required from other State government departments, timelines for setting up of the entire network. The detailed plan shall be also comprised of the scalability, expandability, and security that such architecture will implementation under this project. It is necessary that at least 90% of the proposed last mile connectivity should be wired. Bidder shall also agree to increase the wired connectivity to 100% within 1 year of Go Live. Last Mile to be defined as "the access link from the service provider's PoP – (as per Telco Standards) to the Camera".

1. The Plan should state clearly about the ROW clearances with places having DUCT and cable is laid
2. Places where only duct is available, and cable need to be put in
3. Places where no duct or cable infra s available

A3. Design the LAN connectivity requirements at locations

The successful bidder shall be responsible for gathering the LAN connectivity requirements at the Police locations such as Command centers, Police stations, and other offices. The LAN connectivity may involve setting up the structured cabling, commissioning of active and passive components for operationalization the surveillance system. At present the LAN establishment would be done at the Command Centre, Regional Command Centers, Police Stations, Data Centers/server farm and Picture Intelligence Unit as per user dept requirements

1.3.2 Implementation

B1. Provisioning of connectivity between Cameras, Data Centers, Command Centers and Police Stations

A combination of network technology including leased lines, OFC Network, Terrestrial Networks, Wireless broadband, VSat and Mobile Network technologies is expected to be used to provide seamless connectivity to all cameras. Connectivity to Data Centers and control rooms shall be provided with scalable capacities to allow for expansion in the future. Bidder shall be allowed to procure bandwidth related services from multiple Telecom Service Providers.

Bidders are required to do the estimation of bandwidth & storage requirements considering following benchmark parameters:

Parameter		PTZ Camera	Thermal Camera	Fix Box Camera
Resolution (Min)		1920 X 1080	320 x 240	1920 X 1080
FPS (for Viewing & Storage)	Normal Time	25-30 FPS	15 FPS	25-30 FPS
	No Movement Period / Night Period	15 FPS	8 FPS	15 FPS

Initial monitoring would be done with above mentioned FPS. With advancement of technology, if at the same bandwidth higher resolution can be transmitted, the same shall be adopted. SI shall make available such technological benefits to Govt of Maharashtra, within 120 days of such advancements are available in open market. (Not applicable if the technology is available on proprietary platform.)

- Bidders would need to provide min. 2 MBPS of bandwidth for each Location as per the assessment report of the user dept.
- The actual bandwidth requirement to cater to above mentioned bandwidth & storage parameters and to meet SLAs would be calculated by the bidder and the same shall be clearly proposed in the technical

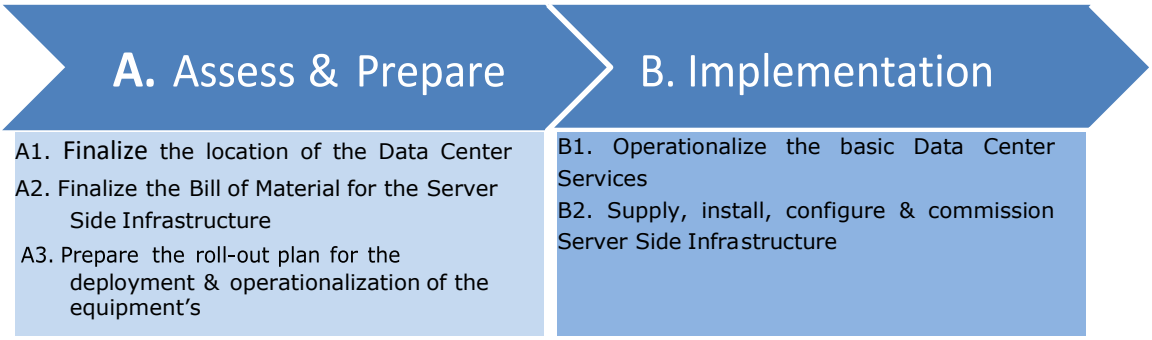
proposal with detail calculations.

- Department also requires the bidder to meet the parameters of video feed quality, security & performance and thus bidders should factor the same while designing the solution.
- GoM reserves its right to ask the Systems Integrator to increase the bandwidth if the provided bandwidth is not sufficient to provide functionality of the system mentioned in the RFP and adhere to the SLAs.

- Bidders are also required to estimate the bandwidth requirement for other connectivity (between Data Centers and Command Centers / viewing Centers) based on the connectivity requirement. The acceptance of the solution would be subject to the proposed networking solution achieving the service e level requirements of the User Department with respect to the Video based Surveillance System. The bandwidth provisioned needs to adhere to the following minimum benchmark requirements –
- Latency should be less than 40 ms.
- Jitter should be less than 10% of one-way latency
- Packet loss should be less than 0.5%

1.4 Implementation of Component #3: Data Centers/server rooms

This Component includes procurement of Server-Side Infrastructure and operationalization of the same at Data Centers & DR in Active – Active mode.



1.4.1 Assess & Prepare

A1. Finalize the location of the Data Centers

It is proposed that the Successful Bidder sets up the entire Server-Side infrastructure in its own Data Center or a Commercial Data Center. This hosting infrastructure is required for both the data centers -

- Data Center 1 (Also called as Primary Data Center)
- Data Center 2 (Also called as Secondary Data Center or Disaster Recovery Center)

Both the Data Centers (Data Center 1 and Data Center 2 should be capable to serve 100% of the cameras but at a given time, each Data Center shall Serve approx. 50% of the cameras, and thus work in Active – Active mode to support the project and act as DR for each other. Redundancy to be provided for all the key components to ensure that no single point of failure affects the performance of the overall system.

Following are the benchmark requirements which should act as guiding factors for the Bidders to propose the locations for these Data Centers.

- Data Center should provide a dedicated rack space for the City Surveillance Project Infrastructure. Racks to be caged.
- Access to the Data Center Space where the City Surveillance Project Infrastructure is hosted should be demarcated and physical access to the place would be given only to the authorized personnel as per access Policy only.

- Indoor CCTV Cameras would be required to be installed to monitor the physic al
- access of the system from remote location
- Data Center 1 & Data Center 2 should be in different seismic zones regions
- Distance between Data Center 1 and Data Center 2 should be minimum of 100 kms.
- Physic al Access to the building hosting Data Centers should be armed and it must be possible to even depute Police personnel for physical security of the premises if felt necessary.

Department would carry out a detail assessment of the proposed locations for the Data Centers on the parameters of Safety & Security and reserves it right to accept or reject the proposed site. In case the proposed site is not acceptable to Department, Successful Bidder shall suggest alternatives matching the requirements mentioned above.

A2. Finalize the Bill of Material for the Server-Side Infrastructure

As part of preparing the final bill of material for the physical data center, the successful bidder will be required to list all passive & active component s required in the data centers. The bill of material proposed by the successful bidder will be approved by City Police for its supply and installation. Indicative equipment's to be commissioned as part of Server-Side infrastructure at Data Centers (Data Center 1 & Data Center 2) are as under:

- Servers (inclusive of OS)
  - Application Servers
  - Recording Server
  - Analytics Server
  - Database Server
  - Management Server
  - Backup Server
  - Domain Controller
  - Any other Server required to the cater to the scope of work mentioned in this
- Application & System Software
  - Video Management System
  - Analytics Software (min. licenses as per requirement estimated in assessment report)
  - Software for Recording, Viewing of Videos
  - Base Map for City
  - RDBMS (if required)
  - Backup Solution
  - Enterprise Management System including SLA Management, Helpdesk Management Network Management & BMS
  - Anti-virus Software
- Customized Software to cater to requirements of Project Requirements
- Primary Storage Solution
- Backup / Secondary Storage Solution
- Storage Management Solution
- Core Router
- Switches (L2 & L3 Switches)
- KVM Switches
- Racks (Caged)
- Fireproof Enclosure for Media Storage (Optional)
- All required Passive Components

The above are only indicative requirements of IT & Non-IT Infrastructure requirements at data centers. The exact quantity and requirement would emerge after the Project Design Document, prepared by the successful bidder, and is approved by GoM. Benchmark specifications for various items mentioned above are given in the Annexure to this RFP document.

A3. Prepare roll-out plan for deployment & operationalization of equipment's

The successful bidder shall prepare the overall Server centers establishment & their operational plan for this project. The plan shall comprise of deployment of all the equipment's required under the project. The implementation roll- out plan for setting up the data centers shall be approved by the City Police. The detailed plan shall be also comprised of the scalability, expandability, and security that such data centers will implementation under this project.

1.4.2 Implementation

B1. Operationalize the basic Data Center Services

Selection of appropriate Data Center and its timely operationalization is critical to maintain project timelines. It is important that the successful bidder gets the cage deployed inside the server farm for this project and prepares the Data Center to install & commission the Server-Side Infrastructure of the project.

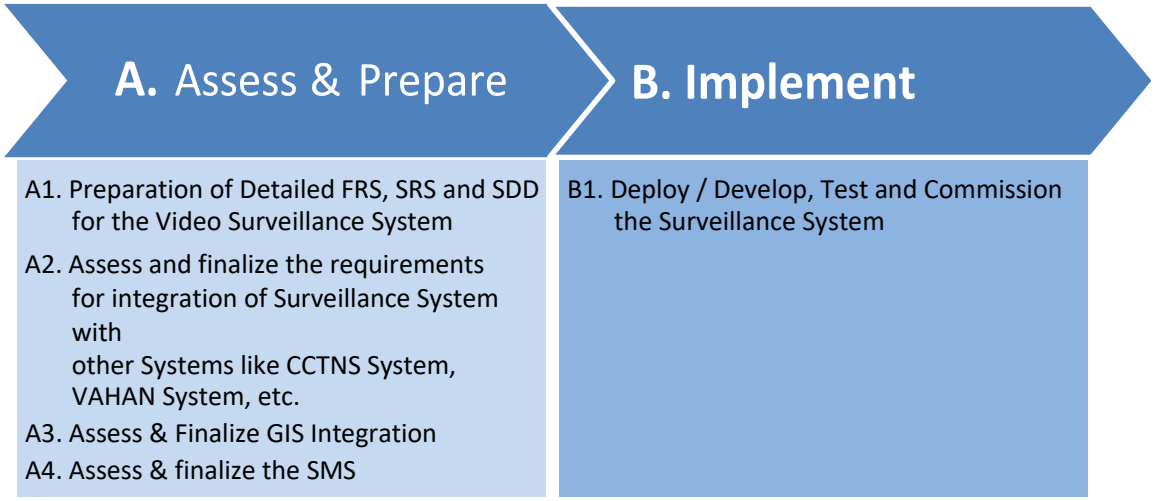
B2. Supply, install, configure & commission Server-Side Infrastructure

The successful bidder shall provide system integration service es to procure and commission the required software and hardware infrastructure at the two Data Centers and deploy the complete surveillance management applications. The SI shall be completely responsible for the sourcing, installation, commissioning, testing and certification of the necessary software licenses and infrastructure required to deploy the Solution at the Data Centers the successful bidder shall be responsible for the provisioning of connectivity from cameras to Data Centers and from data cent res to all the command centers.

The system integrator shall be required to submit a detailed installation report post installation of all the equipment at approved locations. The report shall be utilized during the acceptance testing period of the project to verify the actual quantity of the equipment supplied and commissioned under the project.

1.5 Implementation of Component #4: Application Portfolio

This Component shall include all the necessary applications required for the project such as Video Management System, Recording System, Analytics System, GIS, customized Dashboard (integrated view of relevant sub-system) for various categories of personnel, EMS, etc.



1.5.1 Assess & Prepare

A1. Preparation of Detailed FRS, SRS and SDD for the Video Surveillance System

The present RFP document covers the key expectations from the project. However, it is required that the Successful Bidder document the requirements in detail before the work on execution begins. Following document are expected to be delivered as part of this document:

- **Functional Requirements Document**, giving complete details of the functional aspects of the project. Some of the key functional requirements for designing the system are given in Annexure II.
- **System Requirements document**, giving complete details of the entire system components and their inter relationships to execute the project once operational
- **System Design Document**, detailing out the design of the Surveillance System, Command Control Center in particular, including integration with various systems like Transport Department Systems, CCTNS, etc.

The Successful Bidder should prepare above mentioned document in discussion with all key stakeholders (User Dept, Police Dept, IT Dept, Consultants, etc.) and present it to the CCTV Implementation Committee (User dept, User, Police It is expected that the successful bidder brings on table some International Experience in this field and ensure that a progressive system is implemented for the City Surveillance.

1.5.2 Implementation

B1. Supply, installation, Test and Commission the Surveillance System

The successful bidder will be responsible for the solution deployment / customization for implementing end-to-end surveillance management system including its integration with other systems as mentioned above. The application or COTS will be customized to meet the project objectives and the requirements of City Police e. The bidder will ensure that the Best Practices for Software Development and Customization are used during the software development / customization and implementation exercise. This would at a minimum include:

Software development / customization based on the functional requirement specifications, system requirement specifications, software requirement specifications and solution designs finalized after the approval of City Police. Wherever necessary, the successful bidder shall develop additional functionality/modules to meet the project requirements.

a) Delivering the surveillance management system, along with all the necessary modules and additional functionalities/ integrated COTS products, utilities, system drivers and document consistent with proven standards, including product updates, technology upgrades and patches to run on the selected operating system(s) and hardware according to the solution.
b) Deployment and commissioning of surveillance management system with all the necessary solution elements at the data centers. It is pertinent to mention that application hosted at the data centers shall be accessible by the intended users as desired under this project.
c) Provision for Police officers to login into the system remotely from any location via a secure private network.

Note: Over the period of the contract, even after the Go-Live of the system, department may require certain modifications or additions in the application or the development of new modules. Also, the selected Bidder can suggest certain improvements in the software to make the operations more effective at no additional cost. In such a situation, the selected Bidder shall be responsible for carrying out software enhancement / development activities, as requested by the Department. Any software development / modification will need to pass through the following envisaged phase:

- Conceptualization of solution

- Design
- Development
- Unit and Integration testing
- User acceptance testing
- Roll out/go live

1.6 Implementation of Component #5: Command Centers/server room

This Component would cover deployment of infrastructure (active, passive equipment's) to for various command control Centers & at Police Stations. All camera feeds should be available for viewing by Personnel at any point of time. CP Office Command Center should have simultaneous viewing capability for about 10% of all cameras, 2nd Command Center (which will also act as a DR Command Center to CP Office Command Center) should have viewing capability for 5% of all cameras, Regional viewing Centers should have simultaneous viewing capability for about 10% of cameras of the respective region, DCP/SP level viewing centers should have viewing capability of 10% of respective Zone, Police stations should have simultaneous viewing capability for about 50% of cameras of the respective jurisdiction.

1.6.1.1 Central Control and Command Center

Center to be at project level and at state level for state level project.

1.6.1.2 Broad level Bill of Material required at the Central Control Center at CP/SP office is as follows

IT Components

- Video Wall (percentage of visibility-at any given time 50% of the cameras)
- Monitoring Workstations
- LAN Components

Non-IT Components(based on requirement user dept can decide)

- UPS (adequate Capacity to cover all above IT Components with 30 min. Backup)
- Automatic DG Set to provide power backup for 12 hours to the command center

1.6.1.3 Command Control Center

Broad level Bill of Material required at the 2nd Control Center is as follows:

IT Components

- Video Wall
- Monitoring Workstations
- LAN Components
- UPS (adequate Capacity to cover all above IT Components with 30 min. Backup)
- Automatic DG Set to provide power backup for 12 hours to the command center

Command center will function as viewing centers and shall primarily provide interface to view the video feeds and bring into operation the advanced ANPR. As specified in the SLA table (given in Volume I) ANPR for Roman Number Plates need to have accuracy of more than 90%. These SLA requirements would be revised upwards in case the standardized number plates are implemented by the Government.

1.6.1.4 Broad level Client-side Bill of Material required at each of the regional viewing Centers is as follows:

IT Components

- Video Wall
- Monitoring Workstations
- LAN Components
- UPS (adequate capacity to cover all above IT Components with 30 min. Backup)

1.6.1.5 Zonal Offices

Broad level Bill of Material required at 13 Zonal (DCP) Office level is as follows:

IT Components

- Display Unit
- Workstations
- Adequate LAN Components

1.6.1.6 Police Stations

Broad level Bill of Material required at Police e station level is as follows (numbers calculated for 100 Police e Stations). Deployment plan for each Police e station shall be finalized by SI in consultation with Police Dept:

IT Components

- Display unit
- Workstation
- Adequate LAN Components
- UPS – (adequate capacity to cover all above IT Components with 30min. Backup)

1.6.1.7 Viewing Center at HQ

Broad level Bill of Material required at the viewing Center at HQ is as follows:

IT Components

- Video Wall /Display Unit
- Workstations
- Adequate LAN Components

SI shall provide connectivity to the Viewing Centers at Mantralaya/or location as specified by use dept (+1) for viewing of feeds at thetime of Disaster Management. The bandwidth provisioning to be done by SI for 50 camera feeds from Data Center to viewing centers.

1.7 Implementation of Component #6: Picture Intelligence Unit

Picture Intelligence Unit (PIU) shall be given access to the databases of Passport,CCTNS, Prisons, AMBIS or any similar database available with the State Government. Itshall also create a repository of photographs obtained from various Police sources like Newspapers, Photos during raids, Photos sent by people, etc. Such photographs wouldbe tagged for sex, age, scars, tattoos, etc. so that these become searchable. Some ofthe approaches to be used by the Picture Intelligence Unit for implementation of FacialRecognition System would be as follows:

- Match a suspect / criminal photograph with these databases
- Search photographs from the database meeting certain suspect features

- Match a suspected Criminal face with Video Feeds of specific camera locations orwith the feed received from private or other public organization's video feeds

Whenever there is a requirement at any of the Police Station to check the identity of an individual, Police Station would make such a request to PIU, who in turn would search the databases available with it to match the individual. Such databases would either beaccessed through web services or in a downloaded manner. Full audit trail of reports and data providedwill be maintained.

The successful bidder shall prepare a detail requirement analysis document inconsultation with User Department, Technical Committee, andthe project consultants.

PIU shall oversee the integration of ANPR with the other relevant databases like VAHAN. Further the PIU shall also evaluate the use of various emerging technologies andcustomize these solutions for effective deployments. Such technologies shall include:

- Unidentified object detection
- Motion / intrusion detection
- Noise level detection (gunshot, explosion, shattering of glass etc.)
- Camera Vandalism and tamper detection
- Virtual Fence / Tress Passing / Tripwire
- People / Mass movement
- Car Traffic Events (Start/Stop/Illegal parking/wrong direction/Speed)

SI must provide adequate team to operationalize PIU and train the Police e Personnel to make optimum utilization of the same.

PIU shall be responsible for preparing various guideline document / manuals for theappropriate use of video data and for uniform operationalization of Surveillance systems across the city at different private / public institutions. Indicative list of such guideline document / manuals to be prepared by the PIU is given below:

- Guideline document / manual to standardize file formats, compression types, interfaces, to be used by various agencies (such as Fire Dept, Ambulance Dept, Other Public Institutions, Pvt. Institutions, etc.) concerned with video /photograph recording & storage.
- Guidelines for video data handling for submission of the video data to Judiciary as legal evidence.
- Guideline document / manual for setting up of Video Surveillance S y s t e m by Private and Public institutions within the city.

SI is expected to adhere to the industry best practice & build upon the learning's to improve the performance & accuracy of the system. The core job of PIU would need tobe extended to other cities in the State upon setup of City Surveillance Systems in those respective cities. Successful Bidder is expected to carry out detailed SRS to understand how the CCTNS, VAHAN and any other Police e dept systems can be integrated with the CCTV based City Surveillance System for City.

Broad level Bill of Material for IT / Non-IT Infrastructure required to setup the PictureIntelligence Unit is as follows:

- PCs
- 10 TB Primary Storage
- Adequate User Licenses forthe Facial Recognition System, Data Mining System
- video stream licenses for ANPR
- video stream Licenses for other type of analytics mentioned above

- Hardware, Software for supporting creation of legal evidence on CDs / DVDs in an untampered manner. It is necessary that creating such evidence on CD / DVD / any other storage media is done as per legal requirements so that the evidence is considered as un-tampered in the court of law.
- Connectivity from the Data Center (if housed at different place other than already connected)
- UPS Backup to electronic equipment's for 30 Minutes
- Automatic DG Set to provide power backup for the entire PIU setup for 12 hours

1.8 Implementation of Component #8: Collaborative Monitoring For the purpose of explanation of collaborative monitoring, City Surveillance at publicplaces inthe City is divided into 3categories:

1. **Surveillance System in Direct control of City Police –** Cameras directlyunder the control of City Police and owned by the Government, as setup through the present RFP.
2. **Surveillance System setup by other Public Institutions –** Cameras ownedby and under control of various public institutions like railways, airport, BSE, Passport Office, etc.
3. **Surveillance System setup by Private Institutions –** Cameras owned and controlled by private establishments such as hotels, malls, multiplexes, theatres, hospitals, and schools.

1.9 Provision for integration and availability of Ports and Infra for further integrations

Systems Integrator shall assist user Department in preparation of technical and operative guidelines to be circulated to all stake holders to mandate/ recommend the type of surveillance systems to be deployed and methods to interconnect with the other Surveillance system. Present RFP provides primarily for the scope of work for the system integrator to design, build, and operatethe system for (direct control) with back-end provision to accommodate inputs from systems type 2 and 3 above. Necessary trainings would be organized by the respective organizations for some specific Viewing Staff. Police Department shall facilitate to get co-operation from the private / public establishments for collaborative monitoring duringimplementation & post-implementation. SI would not be responsible for the performance of the system belonging to external agencies.

1.10 Preparation and implementation of the Information security Policy, including Policies on backup

The successful bidder shall prepare the Information Security Policy for the overall project
and the same would be reviewed by the User Department & it's Consultant & then finalized by the User Department. The Security Policy needs to be submitted by the Systems Integrator within 1st quarter of the successful Final Acceptance Tests.

1.11 Training to the Police Personnel for operationalization of the system

Training is an important aspect of this project, and Government expects the successful
bidder to undertake it in a very professional manner. Bidder must conduct a proper Training Needs Analysis of all the concerned staff and draw up a systematic training plan in line with the overall project plan. For all these training programs the bidder must provide necessary course material and reference manuals (user/maintenance/ administration).

Trainings would be of three types:

Functional Training: This training would focus on the use of the surveillance software at Command & Control Rooms, so that the users are aware of all the operations of the surveillance systems and are able to implementation the overall process defined by the PoliceDepartment for optimum use of the system. Broad training requirement defined for the purpose of calculation of effort is as follows –

- Initial training of approx.---------- personnel,

Administrative Training: This training would focus on the administration of Surveillance System and Server Infrastructure and would be imparted to about 8 – 10staff identified by the Government for Administration of the System from Government side. SI shall also provide additional training program of 1 batch (of 8 - 10 personnel) of 5 days every 6 months. Expected training time would be 40 hrs. (5 days of 8 hrs. each).

Senior Management Training: This training would focus on how to use the surveillance system for day-to-day monitoring by the Sr. Management and access various exception reports. Broad training requirement defined for the purpose of calculation of effort is as follows –

- Initial Training of approx. ---------- officers (i.e., about 4 batches of 10 officerseach)

1.12 Final Acceptance Testing of IT& Non-IT Equipment's

The acceptance test for the project shall be carried out in two phases by User Department or duly appointed third party agency by User Department. The Successful bidder should cooperate with the third-party agency to ensure successful completion ofAcceptance tests.

The acceptance test shall consist of Final acceptance test (FAT). The successful bidder shall submit a detailed acceptance testing document at the stage of planning (as mentioned in section 1.1 of this model RFP) and User Department & the successful bidder shall mutually agree upon the same.

1.12.1 Final acceptance Test

After successful installation of equipment's in accordance with the requirements in theRFP, the successful bidder would need to carry out Final Acceptance Testing in 2 different phases - **(a) Unit Testing** and **(b) Integration Testing**. These tests would becarried out based on the test cases developed and validated by User Department and City Police. Apart from the functional testing of the entire system components, thetesting would also verify following aspects – Configuration Testing (to ensure that all the components are configured properly)Security Testing (to review & evaluate security controls)

Final Acceptance Certificate shall be issued by User Department to the successful bidder after successful testing in a real time condition for at least 15 days of trouble-free operation. The date on which final acceptance certificate is issued shall be deemed date of the successful commissioning of the project (either whole or partial, depending upon the implementation strategy adopted). User Department shall consider implementation of 95% cameras as a sufficient condition for the overall project Go-Live. Any delay by the successful bidder in the performance of its contracted obligations shall render the successful bidder liable to the imposition of appropriate liquidated damages, unless agreed otherwise by tenderer.

1.13 System Documents, User Documents

The Successful Bidder will provide document, which h should follow the ITIL (Information Technology Infrastructure Library) standards. This document shouldbe submitted as the project undergoes various stages of implementation. Indicative listof documents include:

- **Project Commencement Document:** Project Plan in giving out micro level activities with milestones & deadlines.
- **Cabling Layout:** Systems Integrator shall submit the detail cabling Layout including cable routing, telecommunication closets and telecommunication outlet/connector designations. The layout shall detail locations of all equipment and indicate all wiring pathways.
- **Equipment Manuals:** Original Manuals from OEMs.
- **Installation Manual:** For all the Application Systems
- **Training Material:** Training Material will include the presentations used for trainings and the required

relevant document forthe topics being covered.

- **User Manuals:** For all the Application Software Modules, required for operationalization of the system.
- **System Manual:** For all the Application Software Modules, covering detail information required for its administration.
- **Operational Manual:** The bidder shall be responsible for preparing OperationalManual relating to operation and maintenance of each service as mentioned in this RFP. The prepared process document shall be formally signedoff by User Department before completion of final acceptance test.

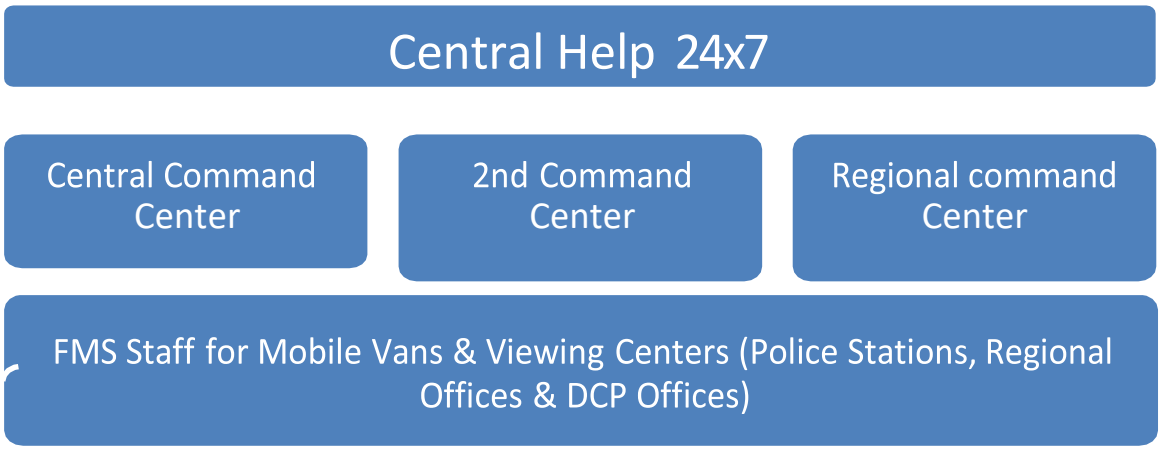
Note: The successful bidder will ensure Upkeep & Updating of all document and manuals during the contractual period. The ownership of all documents, supplied by theSuccessful Bidder, will be with User Department. Document shall be submitted in two copies each in Printed & in Softcopy Formats.

1.14 Post Implementation Services

Success of the project would lie on how professionally and methodic ally the entire project is managed once the implementation is completed. From the Systems Integrator perspective too, this is a critic al phase since 20% of the payment would happen after successful FAT while 80% of the payment towards the project would happen in 20 equal quarterly installments. Successful Integrator thus is required to depute a dedicated team of professionals to manage the project and ensure adherence to the required SLAs.

1.14.1 Helpdesk and Facilities Management Services (Component 9)

The successful bidder will be required to establish the Helpdesk and provide facilities management services to support the Police officials/user dept in performing their day-to-day functions related to this system. Overall structure of the Helpdesk required for the project is as under:



The successful bidder shall setup a central Helpdesk which h shall be supported by their field units, proposed to be setup at command centers and various viewing centers. This Helpdesk would be operational upon implementation of the 1st Command Center.

Functional requirements of the Helpdesk management system, fully integrated with theenterprise monitoring and network management system, is provided in **Annexure 2**.The system will be accessed by the Police e officials for raising their incidents and logging calls for support. The detailed service levels and response time which h the successful bidder is required to maintain for provisioning of the FMS service es are described in the service level agreement of this RFP.

Systems Integrator is also required to depute a dedicated, centralized project management & technical team for the overall project management and interaction withSr. Police Dept / User Dept personnel.

To ensure that there is no downtime for any of the critic al components, the successful Systems Integrator is expected to provision on-site spares and resident engineer(s). Helpdesk Personnel would be located at CP Office CommandCenter.

1.14.2 Planning, Suggesting and Submitting the Surveillance System up-grade plan(s) for five years from the date of acceptance alongwith detailed specifications

As we are aware, constant changes / updates happen in technology, and it is very important that the Surveillance System implemented by the city keeps its pace with the technology. User Department would want the successful bidder to submita report, every 6 months, on the advancements available in technology to make the best use of the existing infrastructure. Any upgradation suggested by the SI would be analyzed by the User Department & it's consultant (if any) and appropriatedecision would be taken.

1.14.3 Hand-over of the system at the end of contractual period along with all documents required to operate and maintain the system

Systems Integrator will supply to the User Department the following before end of 14th Quarter (i.e. min. 6 months prior to the expiry of the contract) :

- Information relating to the current services rendered and data relating to the performance of the services; Entire Document relating to various components of the Project, any other data and confidential information related to the Project.
- All other information (including but not limited to document, records, and agreements) relating to the products & services related to the project to enable User Department and its nominated agencies, or its Replacing Vendor to carry out due diligence to transition the provision of the Project Services to Police e Department or its nominated agencies, or its Replacing Vendor (as the casemay be).
- Capacity Building to be ensured by User department by sharing of list of personnel to be trained to take handover of the project. SI to impart expert level training to all such dept nominated personal as part of exit management plan

1.14.4 Exit Management Plan for CCTV Project - 5 Years After Implementation

The purpose of this Exit Management Plan is to outline the procedures and strategies for the eventual decommissioning or upgrade of the CCTV surveillance project, which is now five years into its operation. This plan aims to ensure a smooth transition, data preservation, and the responsible handling of surveillance equipment.

Exit Management Strategies

1. **Assessment of System Performance:** At the five-year mark, conduct a comprehensive performance assessment of the CCTV system. Identify areas where the system may require upgrades or replacements to meet current security standards.
2. **Cost-Benefit Analysis:** Conduct a cost-benefit analysis to determine whether an upgrade, system replacement, or continuation with the existing system is the most economically viable option.
3. **Stakeholder Engagement**: Consult with key stakeholders, including management, security personnel, and any relevant regulatory bodies, to gain their insights and input on the future of the CCTV system.
4. **Legal and Regulatory Compliance**: Ensure that the system continues to comply with all applicable laws

and regulations, particularly in the context of privacy, data retention, and surveillance licensing.

5. **Data Preservation:** Develop a plan for the preservation and archiving of surveillance data. Ensure that archived data is accessible for any potential future legal or security requirements**.**
6. **Vendor and Supplier Relationships:** Evaluate existing vendor and supplier contracts. Determine whether to renew, renegotiate, or seek new suppliers for equipment and maintenance services.
7. **Personnel Training:** Assess the training needs of personnel responsible for CCTV system operations and maintenance. Ensure that they are up to date with the latest technologies and practices.
8. **Budget Allocation:** Allocate an appropriate budget for upgrades or replacements based on the cost-benefit analysis and the recommendations of the stakeholders**.**
9. **Decommissioning Plan:** Develop a detailed plan for the decommissioning of the existing system if it is to be replaced. This plan should include procedures for safe equipment disposal or recycling.
10. **Project Timeline:** Establish a clear project timeline for the implementation of the exit strategy, whether it involves system upgrades or decommissioning.

Communication and Document

- Maintain clear and comprehensive document of all aspects of the project, including system specifications, maintenance logs, and any legal or regulatory document.
- Keep all stakeholders informed throughout the process, from initial assessment through to final implementation.
- Maintain records of all discussions, decisions, and agreements related to the project exit management.

Responsibilities

- **Project Manager:** Responsible for overseeing the entire exit management process, including budget allocation and stakeholder engagement.
- **Technical Team:** Responsible for the technical aspects, including system assessment, data preservation, and equipment maintenance or replacement.
- **Legal and Compliance Team:** Responsible for ensuring legal and regulatory compliance throughout the exit process.
- **Training Team:** Responsible for personnel training and development.
- **Procurement Team:** Responsible for vendor and supplier evaluations and contract management.

Final Transfer agreement between SI and User Department

2. Responsibility Matrix

The roles of the stakeholders shall change over a period as the project will evolve from design to implementation and enter the operations phase. Stakeholders' responsibilities, illustrative organizational structure for the design & implementation phase, operational phase is given below:

Various Stakeholders identified for City Surveillance Project are as below:

HD User Department

PD City Police Department (Under the leadership of CP)

OS Other Stakeholders (Govt / Semi-Govt Organizations like Railways, MCGM, Airport, BEST, etc.)

Con Project Management Consultant (Need Basis)

SI Systems Integrator (Vendor selected for the Project's Implementation)

Responsibilities are shown using RACI Matrix which h splits project tasks down to four participatory responsibility types that are then assigned to different Stakeholders in the project.

R (Responsible)- Those who do work to achieve the task

A (Approve) - The Stakeholder that ultimately approves the task

C (Consulted)- Those whose opinions are sought (2-way communication)

I (Informed) **-** Those who are kept up to date on progress (1 way communication)

Activity	HD	PD	OS	Con	SI
Signing of the Contract	R	A		A	
Preparation of the Inception Report	R	C		R	
Integrated Plan for the Design & Implementation	R	A		C	
Detailed Technical Architecture	R	C	C	R	
Finalize List of Locations for Edge Devices	R	A		C	
Prepare Detailed Plan for Camera Connectivity	R	A		C	
Prepare FRS, SRS document, Finalize Reporting	R	A		C	
Submission of Final Acceptance	R	A		C	
Supply, Installation, and Commissioning	R	C			A
Supply, Installation of Other Facilities	R	C			A
Provisioning of Connectivity	R	A		C	
Implementing Surveillance System Information	R	C		C	
Preparation of Policy Document	R	C			
Surveillance System for the City	R	C		C	
Guideline Document/Manual for Standardization	R	C		C	
Guidelines for Video Data Handling	R	C		C	
Guideline Document/Manual for Setup of CCTV	R	C		C	
Preparation of Guideline Document for CCTV Feed	R	C		C	
Training and Capacity Building for Police Dept.	R	C		C	
Partial & Final Acceptance Testing of Equipment	R	A		C	A
Planning and Submitting Upgrade Plans	R	A		C	
System and User Document	R	A		C	
Providing Technically Qualified Manpower	R	C		C	
On-Site Facilities Management Service	R	C		C	
Comprehensive Warranty Maintenance	R	C		C	
Provision of On-Site Spares	R	C		C	
Provision of Resident Engineer(s)	R	C		C	
Hand-over of the System	R	C		C	
Weekly Progress Reports	R	I	I	C	C
Monthly Progress Reports	R	I	I	C	C

3. Annexure 1: Common guidelines / comments regarding the compliance of IT / Non-IT Equipment's / Systems to be procured

---

- The specifications mentioned for various IT / Non- IT components are indicative requirements and should be treated for benchmarking purpose only. Bidders are required to undertake their own requirement analysis and may propose higher specifications that are better suited to the requirements.
- Any manufacturer and product name mentioned in the RFP should not be treated as a recommendation of the manufacturer / product.
- None of the IT / Non-IT equipment's proposed by the bidder should be End of Life product. It is essential that the technical proposal is accompanied by the OEM certificate in the format given in Volume I of this RFP, where- in the OEM will certify that the product is not end of life product & shall support for at least 6 years from the date of Bid Submission.
- All IT Components should support IPv4 and IPv6
- Technical Proposal should be accompanied by OEM's product brochure / datasheet. Bidders should ensure complete warranty and support for all equipment from OEMs. All the bac k-to-bac k service e agreements should be submitted along with the Technical Bid.
- All equipment, parts should be Original and New.
- The User Interface of the system should be a User-Friendly Graphical User Interface (GUI).
- Critic al / Core components of the system should not have any requirements to have proprietary Platforms and should conform to open standards.
- For the custom-made modules, Industry standards and norms should be adhered to for coding during application development to make debugging and maintenance easier. Object oriented programming methodology must be followed to facilitate sharing, componentizing, and multiple use of standard code. The application should be subjected to Application security audit to ensure that the application is free from any vulnerability, before hosting the application by any of the CERTIN empaneled vendors.
- All the Clients Machines / Servers shall support static assigned IP addresses or shall obtain IP addresses from a DNS/DHCP server.
- The Successful Bidder should also propose the specifications of any additional servers / other hardware, if required for the system.
- The indicative architecture of the system is given above. The Successful Bidder must provide the architecture of the solution it is proposing.
- The system servers and software applications will be hosted in Data Center identified by the Successful Bidder. It is important that the entire set of Data Center equipment's are in safe custody and have access from only the authorized personnel and should be in line with the requirements & SLAs defined in the RFP.
- The Servers provided should meet industry standard performance parameters. In case any non-standard computing environment is proposed (such as cloud), detail clarification needs to be provided to confirm a) how the sizing has been arrived at and b) how SLAs would be met.SI is required to ensure that there is no choking point / bottleneck anywhere in the system (end-to-end) to affect the performance / SLAs.
- All the hardware and software supplied should be from the reputed Original Equipment Manufacturers (OEMs). User Department reserves the right to ask replacement of any hardware / software if it is not from a reputed brand and conforms to all the requirements specified in the tender document.
- All Servers, Active Networking Components (for Edge Level Switches, please refer below for additional information), Security Equipment, Storage Systems and COTS Application proposed should be from OEMs who are amongst the top 5 for World- wide Market share in terms of Revenue as per Gartner / IDC latest

published quarterly report. Bidder is expected to attach the report along with the technical proposal.

- Cameras and the Video Management / Video Analytic s Software should be ONVIF Core Specification '2.X' or 'S' compliant and provide support for ONVIF profiles such as Streaming, Storage, Recording, Playback, and Access Control.
- System Integrator shall place orders on various OEMs directly and not through any sub-contractor / partner.
- All licenses should be in the name of User department, Govt of Maharashtra.

- Following selection criteria are to be followed for OEMs for cameras, VMS, ANPR & other analytic s:

Component	Proposed Selection Criteria for OEM
Surveillance Cameras	Minimum installation base of 50,000 IP based cameras across globe as on 31/03/2023 and Should have been operational for at least 2 City Surveillance projects (globally) of minimum 1000 IP based cameras each in last 5 years OR IMS World Report for Network Security Cameras, Report for Security Cameras & Report for Intelligent Cameras
Video Management Software	Minimum installation base of 50 projects across globe as on 31/03/2023 and Should have been operational for at least 2 City Surveillance projects (globally) of minimum 1000 cameras each in last 5 years OR IMS World Report for Video Management Software
ANPR Cameras	Minimum installation base of 5,000 cameras across globe as on 31/03/2023 and Should have been operational for at least 2 City Surveillance projects (globally) for supporting minimum 100 ANPR cameras each in last 5 years OR IMS World Report for ANPR Camera
Thermal Cameras	Minimum installation base of 1,000 cameras across globe as on 31/03/2023 and Should have been operational for at least 2 City Surveillance projects (globally) for supporting minimum 30 Thermal cameras each in last 5 years OR IMS World Report for Thermal Cameras
Other Analytics	Minimum installation base of 5,000 cameras across globe and Should have been operational for at least 2 City Surveillance projects (globally) of minimum 500 cameras each in last 5 years OR IMS World Report for Video Analytic s

Edge Level Switch	Minimum installation base of 5,000 switches across globe as on 31/03/2023 and Should have been operational for at least 2 City Surveillance projects (globally) for supporting minimum 1000 cameras each in last 5 years

With regards to above, OEMs will certify the installation base and the project experience. This certificate shall be issued through the Global Headquarters and attested by the Indian office. Tendering authority shall verify the claim of OEMs by using publicly available reports like IMS, in case there is any doubt of gross negligence. Decision of GoM shall be final and binding upon the Bidder and OEM.

4. Annexure 2: Functional Requirements for the Proposed Surveillance System

Functional Requirement of the overall Surveillance System can be categorized into following components:

- Information to be Captured by Edge Devises
- Information to be Managed at the Command Centers
- Information to be made available to different Police Personnel
- Operational Requirements
- Storage / Recording Requirements
- Other General Requirements

Detailed requirement finalization will be done during pre- implementation stage.

4.1 Information to be Captured by Edge Devises

Cameras being the core of the entire Surveillance system, it is important that their selection is carefully done to ensure suitability & accuracy of the information captured on the field and is rugged, durable & compact. These cameras need to work on 24 X 7 basis and transmit quality video feeds to the centralized data centers and would capture the video feeds at 25 FPS for majority of the time and at 15 FPS for the lean period*. However, user Department shall take the regular review of the requirements for video resolution, FPS and may change these numbers to suit certain specific requirements (for example, there could be a situation when certain cameras are required to be viewed at higher FPS for specific period. It is estimated that not more than 0.5% of the cameras would be required to be viewed at higher FPS at a given point of time).

4.2 Information to be Analyzed at the Command Centers

The proposed Video Management System should provide a complete end-to-end solution for security surveillance application. The control center shall allow an operator to view live / recorded video from any camera on the IP Network. The combination of control center and the IP Network would create a virtual matrix, which h would allow switching of video streams around the system.

As informed in the tender, not all the cameras would be simultaneously viewed at Command Control Centers or at Police e Stations. PIU shall from time to time take decisions on utilization of Alerts / Exceptions / Triggers generated by cameras and specify the client machines where these would get populated automatically.

Police personnel shall have followed access to the video feeds of the cameras of their jurisdiction:

- Viewing rights to all the live Camera Feeds
- Viewing rights to the stored feeds, stored on Primary / Secondary Storage

- Access to view Alerts / Exceptions / Triggers raised (as per requirements defined by PIU from time to time)
- Trail Report on specific person / object / vehicle for a specific period / location
- Personalized Dashboard (depending upon grade of Police e officer)
- Accessibility to advanced analytics on recorded footages (as per requirements defined by PIU from time to time)
- Provide search of recorded video. Advanced search should be possible based on various filters like alarm / event, area, camera, etc.

4.3 Information to be made available to different Police Stations

Various Police Stations shall be given viewing rights of the feeds of the corresponding cameras from the respective Police e Stations. PIU shall take appropriate decisions to provide Alerts / Exceptions / Triggers of the cameras automatically on the client machine made available to Police e Stations. Police personnel shall have followed access to the video feeds of the cameras of their jurisdiction:

- Viewing rights to all the live Camera Feeds
- Viewing rights to the stored feeds, stored on Primary / Secondary Storage
- Access to view Alerts / Exceptions / Triggers raised (as per requirements defined by PIU from time to time)
- Trail Report on specific person / object / vehicle for a specific period / location
- Personalized Dashboard (depending upon grade of Police e officer)

4.4 Role Based Access to the Entire System

Various users should be accessing the system using single sign on and should be role based. Different roles which could be defined (to be finalized at the stage if SRS) could be Administrator, Supervisor, Officer, Operator, etc. Apart from role-based access, the system should also be able to define access based on location. Other minimum features required in the Role Based authentication Systems are as follows:

- The Management Module should be able to capture basic details (including mobile number & e mail id) of the Police Personnel & other personnel requiring Viewing / Administration rights to the system. There should be interface to change these details, after proper authentication.
- Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access.
- Biometric authorization coupled with login name & password should be enabled to ensure that only the concerned personnel can login into the system.
- Surveillance System should have capability to map the cameras to the Police Personnel from different Police Stations. There should be interface to change these mappings too.
- For PTZ cameras, there should be provision to specify hierarchy of operators / officers for control of the cameras from various locations.

4.5 Storage / Recording Requirements

Following are the storage / recording requirements visualized for the City Surveillance system. However, the storage solution should be modular enough to ensure compliance to the changes in storage / recording Policy, to be evolved upon initial deployment of the system.

- 30 days of storage on the Primary Storage for all camera feeds
- Primary storage at each of the Data Centers to have 100% capacity for xxx cameras
- 180 days of storage for ANPR camera feeds & 30 days of storage for other camera feeds on secondary storage (i.e., total storage of 180 days for ANPR camera feeds & 30 days for other cameras feeds)
- Indoor Camera feed/recording to be stored for at least 18 months.

- Secondary storage to be kept at the respective Data Center (i.e., approx. 50% of the
- total camera storage on the secondary storage at both the data centers).
- Secondary Storage (Archival/Backup) can be on any media such as Tapes, Disks, Disk systems, etc. or its combination.
- Data on Primary & Secondary Storage would be over-written automatic ally by newer data after the stipulated time. If some data is flagged by Police personnel (or by designated personnel) as important data / evidence data due to some reporting of crime in the area or due to court order or due to suspicious activity, it would need to be stored for longer duration, as per requirements. Police Committee would analyze such flagged data every 3 months to take such decisions for preservation of the flagged data beyond 90 / 180 days on secondary storage.
- Full audit trail of reports and data provided by PIU to be maintained for 90 days.
- Please refer annexures for specifications for Primary & Secondary Storage.
- Retrieval time for any data stored on secondary storage should be max. 4 hours for critic al data & 8 hours for other data.
- The Recording Servers / System, once configured, shall run independently of the Video Management system and continue to operate in the event that the Management system is off-line.
- The system shall support the use of separate networks, VLANs or switches for connecting the cameras to the recording servers to provide physical network separation from the clients and facilitate the use of static IP addresses for the devices.
- The system shall support H.264/H.265, MPEG-4 and MJPEG compression formats for all analog cameras connected to encoders and all IP cameras connected to the system. The system shall record the native frame rate and resolution supplied by the camera or as configured by the operator from the System Administration Server.
- The system should not limit amount of storage to be allocated for each connected device. The on- line arc hiving capability shall be transparent and allow Clients to browse and arc hive recordings without the need to restore the archive video to a local hard drive for access.
- The system shall allow for the frame rate, bit rate and resolution of each camera to be configured independently for recording. The system shall allow the user to configure groups of cameras with the same frame rate, bit rate and resolution for efficient set-up of multiple cameras simultaneously.
- The system shall support Archiving or the automatic transfer of recordings from a camera's default database to another location on a time-programmable basis without the need for user action or initiation of the archiving process. Archiving shall allow the duration of the camera's recordings to exceed the camera's default database capacity. Archives shall be located on either the recording server or on a connected network drive. If the storage area on a network drive becomes unavailable for recording the system should have the ability to trigger actions such as the automatic sending of email alerts to necessary personnel.
- Bandwidth optimization
    - The Recording Server / System shall offer different codec (H.264, MJPEG, MPEG- 4, etc.) and frame rate (CIF, 4CIF, QCIF) options for managing the bandwidth utilization for live viewing on the Client systems.
    - From the Client systems, the user shall have the option of having video images continually streamed or only updated on motion to conserve bandwidth between the Client systems and the Recording Server.
- The Recording Server / System shall support Camera (analogue and IP cameras) devices from various manufacturers.

- The Recording Server / System shall support the PTZ protocols of the supported
- devices listed by the camera OEMs.
- The system shall support full two-way audio between Client systems and remote devices. (To make the provision for Public Address System (PA) in the future.)
- Failover Support
  - The system shall support automatic failover for Recording Servers. This functionality shall be accomplished by Failover Server as a standby unit that shall take over if one of a group of designated Recording Servers fails. Recordings shall be synchronized back to the original Recording Server once it is back online.
  - The system shall support multiple Failover Servers for a group of Recording Servers.
- SNMP Support
  - The system shall support Implementation Network Management Protocol (SNMP) for third-party software systems to monitor and configure the system.
  - The system shall act as an SNMP agent which h can generate an SNMP trap because of rule activation in addition to other existing rule actions.

4.6 Other General Requirements

Management / Integration functionality

- The Surveillance System shall be a fully distributed solution, designed for large multi- site and multiple server installations requiring 24/7 surveillance. The solution shall offer centralized management of all devices, servers, and users.
- The Surveillance System should not have any limit on the number of cameras to be connected for Surveillance, Monitoring, and recording. Any increase in the no. of cameras should be possible by aug of Hardware components.
- The Surveillance System shall support distributed viewing of any camera in the system using Video walls or big screen displays.
- The Surveillance System shall support alarm management. The alarm management shall allow for the continuous monitoring of the operational status and event- triggered alarms from system servers, cameras, and other external devices.
- It should be possible to integrate the Surveillance System with 3rd-party software, to enable the users to develop customized applications for enhancing the use of video surveillance solution. For e.g., integrating alarm management to initiate SMS, E-Mail, VoIP call etc.
- The Management system shall store the overall network elements configuration in central database, either on the management server computer or on a separate DB Server on the network.

System Administration functionality

- The System Administration Server shall provide a feature-rich administration client for system configuration and day-to- day administration of the system.
- The System Administration Server shall support different logs related to the Management Server.
  - The System Log
  - The Audit Log
  - The Alert Log
  - The Event Log

- Rules

  The system shall support the use of rules to determine when specific actions occur. Rules shall define what actions shall be carried out under specific conditions. The system shall support rule-initiated actions such as:
  - Start and stop recording
  - Set non-default live frame rate
  - Set non-default recording rate
  - Start and stop PTZ patrolling
  - Send notifications via email
  - Pop-up video on designated Client Monitor recipients

Client system

The Client system shall provide remote users with rich functionality and features as described below.

- Viewing live video from cameras on the surveillance system
- Browsing recordings from storage systems
- Creating and switching between multiple of views.
- Viewing video from selected cameras in greater magnification and/or higher quality in a designated hotspot.
- Controlling PTZ cameras.
- Using digital zoom on live as well as recorded video.
- Using sound notifications for attracting attention to detected motion or events.
- Getting quick overview of sequences with detected motion.
- Getting quick overviews of detected alerts or event s.
- Quickly searching selected areas of video recording for motion (also known as Smart Search).

Remote Web Client

a) The web-based remote client shall offer live view of up to 16 cameras, including PTZ control and event / output activation. The Playback function shall give the user concurrent playback of multiple recorded videos with date, alert sequence or time searching.

b) User Authentication – The Remote Client shall support logon using the username and password credentials.

c) App based or QR code-based access system

Matrix Monitor

a) Matrix Monitor – The Matrix Monitor feature shall allow distributed viewing of multiple cameras on the system on any monitor.

b) The Matrix Monitor feature shall access the H.264-265/MJPEG/MPEG4 stream from the connected camera directly and not sourced through the recording server. (Including backward compatibility)

Alarm Management Module

c) The alarm management module shall allow for continuous monitoring of the operational status and event-triggered alarms from various system servers, cameras, and other devices. The alarm management module shall provide a real-time overview of alarm status or technical problems while allowing for immediate visual verification and troubleshooting.

d) The alarm management module shall provide interface and navigational tools through the client including.

   i. Graphical overview of the operational status and alarms from servers, network cameras and external devices including motion detectors and access control systems.

   ii. Intuitive navigation using a map-based, hierarchical structure with hyperlinks to other maps, servers, and devices or through a tree-viewformat.

e) The module shall include flexible access rights and allow each user to be assigned several roles where each shall define access rights to cameras.

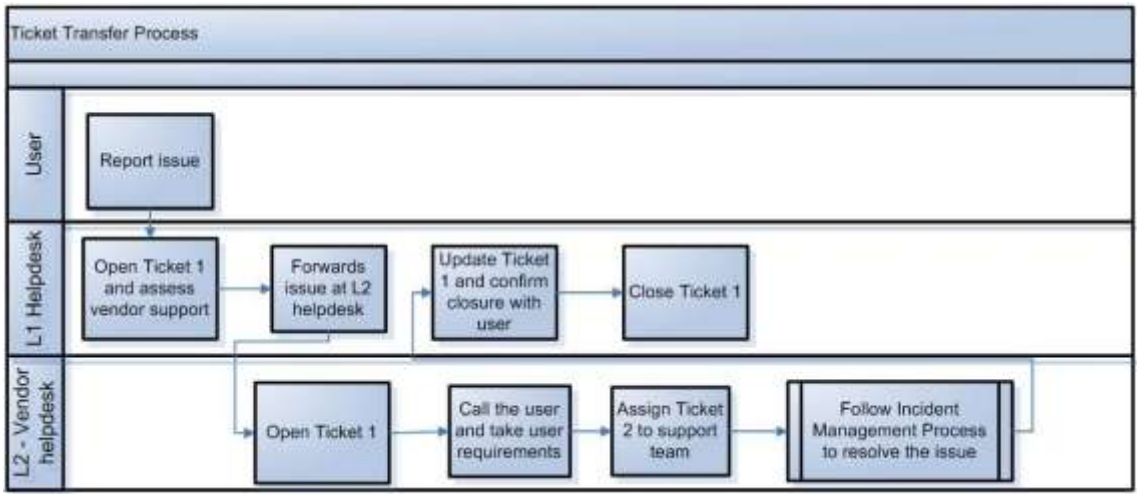
f) Basic VMS should be capable to accept third party generated events / triggers

4.7 Helpdesk Management

It is envisaged that the centralized Helpdesk, functioning as proposed below, would be managed by the Systems Integrator, and shall serve following objectives:

- Act as the Point of Contact for the users of Surveillance System
- Own an Incident throughout its Lifecycle
- Communicate effectively with Police / User Dept Officers and IT support teams.
- Maintain high user satisfaction levels
- Maintain the SLA statistic s & submit quarterly report to Police / User Department

A general process flow for the Helpdesk management is depicted in the flow-chart given as follows. Systems Integrator shall prepare a detailed Helpdesk Policy in consultation with the User Department & its Consultant prior to the Go Live date.



System Integrator shall deploy a State-of-Art Enterprise Management System to handle the complexity of Operations & SLA Management defined in the RFP. Benchmark specifications for the Enterprise Management System is given in subsequent Annexure.

5. Annexure 3 - Surveillance Equipment Technical Specifications

1. Fixed Box cameras (High Definition)

#	Parameter	Minimum Specifications or better
1.	Video Compression	H.264
2.	Video Resolution	1920 X 1080**
3.	Frame rate	Min. 25 fps
4.	Image Sensor	1/3” Progressive Scan CCD / CMOS
5.	Lens Type	Varifocal, C/CS Mount, IR Correction
6.	Lens#	Auto IRIS 8 – 40 mm, F1.4
7.	Minimum Illumination	Color: 0.5 lux, B/W: 0.1 lux (at 30 IRE)

8.	IR Cut Filter	Automatically Removable IR-cut filter
9.	Day/Night Mode	Color, Mono, Auto
10.	S/N Ratio	≥ 50 dB
11.	Auto adjustment + Remote Control of Image settings	Color, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Wide Dynamic Range
12.	Audio	Audio Capture Capability
13.	Local storage	Memory card slot availability
14.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, QoS
15.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption
16.	Operating conditions	0 to 50°C
17.	Casing	NEMA 4X / IP-66 rated
18.	Certification	UL / CE / FCC / EN

2. Pan, Tilt and Zoom cameras (PTZ)

#	Parameters	Minimum Specifications or better
1.	Video Compression	H.264
2.	Video Resolution	1920 X 1080
3.	Frame rate	Min. 25 fps
4.	Image Sensor	1/3" OR ¼" Progressive Scan CCD / CMOS
5.	Lens	Auto-focus, 4.7 - 84.6 mm (corresponding to 18x)
6.	Minimum Illumination	Color: 0.5 lux, B/W: 0.1 lux (at 30 IRE)
7.	Day/Night Mode	Color, Mono, Auto
8.	S/N Ratio	≥ 50dB
9.	PTZ	Pan: 360° endless/continuous, 0.2 to 300°/s (auto), 0.2 to 100°/s (Manual) Tilt: 90°, 0.2 to 100°/s (Auto), 0.2 to 40°/s (Manual) 18x optical zoom and 10x digital zoom 64 preset positions Auto-Trac king Pre-set tour
10.	Auto adjustment + Remote Control of Image settings	Color, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Wide Dynamic Range
11.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, QoS
12.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption
13.	Operating conditions	0 to 50°C
14.	Casing	NEMA 4X / IP-66 rated
15.	Certification	UL / CE / FCC / EN

3. Thermal Cameras

#	Parameter	Minimum Specifications
1.	Video Compression	MJPEG, MPEG-4 / H.264
2.	Resolution	320 X 240
3.	Thermal Sensor	320 X 240 pixels Focal Plan Array (FPA), uncooled Vanadium Oxide (VOx) /Amorphous Silicon Microbolometer
4.	Thermal Sensitivity	50 mK or better
5.	Pan and Tilt	Pan: 360°; 0.2° to 60°/s Tilt: 120° range; 10° to 50°/s Optical Zoom: 26x
6.	Lens	Minimum 80 mm
7.	Detection Range	Should detect an object of size 2.5m X 2.5m up to 4 km
8.	Minimum Illumination	Suitable for pitch-dark conditions (Zero Lux)
9.	Casing	NEMA 4X / IP-66 rated
10.	Operating conditions	-5° to 50°C
11.	Certification	UL / CE / FCC / EN

4. Infrared Illuminators

The infrared illuminators are to be used in conjunction with the Fix Box / PTZ cameras specified above to enhance the night vision.

#	Parameter	Minimum Specifications or better
1.	Range	Min. 100 mtrs
2.	Minimum Illumination	High sensitivity at Zero Lux
3.	Power	Automatic on/off operation
4.	Casing	NEMA 4X / IP-66 rated
5.	Operating conditions	-5° to 50°C
6.	Certification	UL / CE / FCC / EN

Fixed Dome Camera for Indoor Surveillance

#	Parameter	Minimum Specifications
1.	Video Compression	H.264
2.	Video Resolution	1920x1080
3.	Frame rate	25 fps in all resolutions
4.	Image Sensor	1/4” / 1/3” Progressive Scan CMOS
5.	Lens Type	Varifocal, C/CS Mount, IR Correction
6.	Lens	Fixed IRIS 2.8-10mm, F1.7, 10x digital zoom
7.	Minimum Illumination	0.9 lux

8.	Image settings	Compression, Color, brightness, sharpness, contrast, whitebalance,exposure control, backlight compensation, rotation
9.	Protocol	HTTP, HTTPS, FTP, SMTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, QoS
10.	Security	Password Protection, IP Address filtering, User Access Log
11.	Operating conditions	0 to 50°C
12.	Casing	Tamper Resistant casing for Indoor Environment

1. Application / Database/ Recording / Viewing / Other Servers

#	Parameter	Minimum Specifications
1.	Processor	Latest series/ generation of 32 bit or 64-bit x86/RISC/EPIC/CISC processor(s) with Dual (or higher) Cores
2.	RAM	Minimum 32 GB Memory
3.	Internal Storage	300 GB SAS / SATA (15k rpm) disk
4.	Network interface	Dual Integrated Gigabit Ethernet ports (Minimum 2 Integrated Gigabit Ethernet ports) Optional: Fiber channel adapter (if required)
5.	Power supply	Dual Redundant Power Supply
6.	RAID support	As per requirement/solution
7.	Operating System	Licensed version of 32/64 bit latest version of Linux/ Unix/Microsoft® Windows based Operating system, matching with the processor(s) (i.e., 64-bit processor server to have 64-bit OS)
8.	Form Factor	Rack mountable/ Blade

2. Online UPS

S. No.	Parameter	Minimum Specifications
1.	Capacity	Adequate capacity to cover all above IT Components at respective location
2.	Output Wave Form	Pure Sine wave
3.	Input Power Factor at Full Load	>0.90
4.	Input	Three Phase 3 Wire for over 5 KVA
5.	Input Voltage Range	305-475VAC at Full Load
6.	Input Frequency	50Hz +/- 3 Hz

7.	Output Voltage	400V AC, Three Phase for over 5 KVA UPS
8.	Output Frequency	50Hz+/- 0.5% (Free running); +/- 3% (Sync. Mode)
9.	Inverter efficiency	>90%
10.	Overall AC-AC Efficiency	>85%

S. No.	Parameter	Minimum Specifications
11.	UPS shutdown	UPS should shutdown with an alarm and indication on following conditions 1) Output over voltage 2) Output under voltage 3) Battery low 4) Inverter overload 5) Over temperature 6) Output short
12.	Battery Backup	30 minutes in full load
13.	Battery	VRLA (Valve Regulated Lead Acid) SMF (Sealed Maintenance Free) Battery
14.	Indicators & Metering	Indicators for AC Mains, Load on Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc. Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.
15.	Audio Alarm	Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.
16.	Cabinet	Rack / Tower type
17.	Operating Temp	0 to 50 degrees centigrade

3. Primary Storage

#	Parameter	Minimum Specifications
1.	Solution/Type	Bidder is expected to provide NAS / Scale-out NAS / SAN / Unified or equivalent storage solution meeting benchmark performance parameters specified in SLA Solution proposed should yield low cost per TB, while meeting the performance parameters
2.	Storage	Disks should be preferably dual coated Disks should be preferably of 3 TB / 4 TB / higher capacity 30 days of storage on the Primary Storage for all camera feeds To store video stream and other data as required, to meet the archival requirement for different type of video feeds Primary storage to have 100% capacity for all cameras of the project The storage design must be based on the expected data volume from the project, including the expansion requirement of 5 years (System capable of scaling vertically (Controller) & horizontally (disk capacity))
3.	Hardware Platform	Rack mounted form-factor Modular design to support controllers and disk drives expansion

4.	Controllers	At least 2 numbers of Controllers in active/active mode The controllers / Storage nodes should be upgradable seamlessly, without any disruptions / downtime to production workflow for performance, capacity enhancement and software / firmware upgrades.
5.	RAID support	Should support various RAID levels
6.	Redundancy and High Availability	The Storage System should be able to protect the data against single point of failure with respect to hard disks, connectivity interfaces, fans, and power supplies
7.	Management software	All the necessary software to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots etc. Should also include storage performance monitoring and management software Should provide the functionality of proactive monitoring of Disk drive and Storage system for all possible disk failures Should be able to take "snapshots" of the stored data to another logical drive for backup purposes
8.	Data Protection	The storage array must have complete cache protection mechanism either by de-staging data to disk or providing complete cache data protection with battery backup for up to 4 hours

Note:

Storage for PIU

- Bidder to also provide additional Storage of Min10 TB at PIU level as local memory for research purpose. Bidder to provide SAN / NAS / equivalent Storage Solution for this purpose. This solution also to be considered in the SLA for Storage.

4. Secondary Storage

#	Parameter	Minimum Specifications
1.	Solution/Type	Secondary Storage (Archival/Backup) can be on any media such as Tapes, Disks, Disk systems, etc. or its combination. (so as to arrive at lower cost per TB) May or may not use de-duplication technology Compatible with primary storage (at DC1 and DC2)
2.	Backup Size	To store data as required, to meet the archival requirement for different type of video feeds, as follows: 180 days of storage for ANPR camera feeds & 30 days of storage for other camera feeds on secondary storage (these days inclusive of 7 days of primary storage)
3.	Hardware Platform	Rack mounted, Rack based Expansion shelves
4.	Software Platform	Must include backup/arc hive application portfolio required

5.	Retrieval time	Retrieval time for any data stored on secondary storage should be max. 4 hours for critical data & 8 hours for other data. This would be considered for SLA calculation. (Critic al data means any data needing urgent attention by the Judicial System or by Police Dept for investigation / terrorist treat perception). Every incidence of this SLA not being met would be charged a penalty of Rs. 10,000/-. If there is loss within the required period of 30/183 days, there will be an additional penalty of Rs. 500000 /- per instance.

5. Database Licenses

- Bidder needs to provide Licensed RDBMS, enterprise/full version as required for the proposed Surveillance System and following all standard industry norms for performance, data security, authentication and database shall be exportable into XML.

6. Backup Software

- The software shall be primarily used to back up the video feed from the servers onto SAN and backup tapes (when required). The other data that would require backing up would include the various databases that shall be created for the surveillance system. Details of data that would be created are available in the table at section 'Data Requirements'
- Scheduled unattended backup using Police y-based management for all Server and OS platforms
- The software should support on-line backup (transparent to the real time operations of the system) and restore of various applications and Databases
- The backup software should be capable of having multiple back-up sessions simultaneously
- The backup software should support different types of backups such as Full back up, Incremental back up, Differential back up, Selective back up, Point in Time back up and Progressive incremental back up
- The backup software should support different types of user interface such as GUI, Web-based interface

7. Anti-virus Software

- Shall be able to scan through several types of compression formats.
- Must update itself over internet for virus definitions, program updates etc. (periodic ally as well as in push-updates in case of outbreaks)
- Able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)
- Shall be able to scan only those file types which h are potential virus carriers (based on true file type)
- Shall be able to scan for HTML, VBScript Viruses, malicious applets, and ActiveX
- controls
- Shall provide Real-time product Performance Monitor and Built -in Debug and Diagnostic tools, and context- sensitive help.
- The solution must support multiple remote installations
- Shall provide for virus notification options for Virus Outbreak Alert and other configurable Conditional Notification.
- Should be capable of providing multiple layers of defense
- Shall have facility to clean, delete and quarantine the virus affected files.
- Should support scanning for ZIP, RAR compressed files, and TAR arc hive files
- Should support online update, whereby most product updates and patches can be performed without bringing messaging server off-line.
- Should use multiple scan engines during the scanning process

- Should support in- memory scanning to minimize Disk IO.
- Should support multi-threaded scanning
- Should support scanning of nested compressed files
- Should support heuristic scanning to allow rule-based detection of unknown viruses
- Updates to the scan engines should be automated and should not require manual intervention
- All binaries from the vendor that are downloaded and distributed must be signed
- and the signature verified during runtime for enhanced security
- Updates should be capable of being rolled back in case required
- File filtering should be supported by the proposed solution; file filtering should be based on true file type.
- Should support various types of reporting formats such as CSV, HTML, and text files
- Shall scan at least HTTP, FTP traffic (sending & receiving) in real time and protect against viruses, worms & trojan horse attacks and other malicious code.

8. Enterprise Management System

The Enterprise Management System (EMS) is an important requirement of this Project. Various key components of the EMS are:

- SLA & Contract management System
- Network Monitoring System
- Server Monitoring System
- Helpdesk System

- **SLA & Contract management System**

  The SLA & Contract Management solution should enable the User / Police Department to capture all the System based SLAs defined in this RFP and then calculate quarterly (or for any duration) penalty automatically. Measuring service performance requires incorporation of a wide variety of data sources of the Surveillance project. The SLA solution should support the collection data from various sources to calculate Uptime / Performance / Security SLAs. Various features required in this component to EMS are -

  - It must be a centralized monitoring solution for all IT assets (including servers, network equipment's etc.)
  - The solution must have integrated dashboard providing view of non-performing components / issues with related to service e on any active components
  - The solution must follow governance, compliance, and content validations to improve standardization of service level contracts.
  - Application should be pre-configured to allow the users to generate timely reports on the SLAs on various parameters.
  - The solution must support Service e Level Agreements & Lifecycle Management including Version Control, Status Control, Effectively and audit Trail to ensure accountability for the project.
  - The solution must have the ability to define and calculate key performance indicators from an End-to-End Business Service delivery perspective related to Surveillance Project under discussion.
  - The solution should support requirements of the auditors requiring technical audit of the whole system
  - The solution most have an integrated dashboard, view of Contract Parties & current SLA delivery levels and view of Services & current SLA performance
  - The solution should support SLA Alerts escalation and approval process.
  - Solution should support effective root cause analysis, support capabilities for investigating the root causes of failed service levels and must make it possible to find the underlying events that cause the service level contract to fail.

- Accept Data from a variety of formats, provide pre-configured connectors and adapters, Ability to define Adapters to data source in a visual manner without coding.
- Support for Defining and Calculating service Credit and Penalty based on clauses in SLAs.

Reporting

- Ability to generate reports on penalty and credit due, to check on non-compliance of SLAs for the surveillance project.
- Monetary penalties to be levied for non-compliance of SLA, thus the system must provide Service Level Performance Report over time, contract, service e and more.
- The solution should provide historic al and concurrent service e level reports for the surveillance project to ensure accountability of the service e provider's performance.
- Automatic Report creation, execution, and Scheduling, must support variety of export formats including Microsoft Word, Adobe PDF etc.
- The solution must support Templates for report generation, Report Filtering and Consolidation and Context sensitive Drill-down on specific report data to drive standardization and governance of the surveillance project.
- The solution must support security for drill-down capabilities in dashboard reports ensuring visibility for only relevant personnel of the surveillance project
- Support real-time reports (like at-a-glance status) as well as historical analysis reports (like Trend, TopN, Capacity planning reports etc.)
    - Resource utilization exceeding or below customer-defined limits
    - Resource utilization exceeding or below predefined threshold limits

An indicative List of SLAs that needs to be measured centrally by SLA contract management system are given in the RFP document. These SLAs must be represented using appropriate customizable reports to ensure overall service delivery.

- **Network Management System**

Solution should provide fault & performance management of the entire datacenter infrastructure and should monitor IP\SNMP enabled devices like Routers, Switches, Cameras, etc. Proposed Network Management shall integrate with SLA & Contract Management system to supply KPI metrics like availability, utilization to measure central SLA's and calculate penalties. Following are key functionalities that are required which h will help measuring SLA's as well as assist administrators to monitor network faults & performance degradations to reduce downtimes, increase availability and take proactive actions to remediate & restore network services.

- The proposed solution must automatic ally discover manageable elements
- connected to the infrastructure and map the connectivity between them. Solution should provide centralized monitoring console displaying network topology map from central location to Zonal / Police e Station Level.
- Proposed solution should provide customizable reporting interface to create custom reports for collected data.
- The system must use advanced root-cause analysis techniques and Policy-based condition correlation technology for comprehensive analysis of infrastructure faults.
- The system should be able to clearly identify configuration changes as root cause of network problems and administrators should receive an alert in case of any change made on routers spread

across surveillance project.

- Network Performance management system should provide predictive performance monitoring and should be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits based on baseline data instead of setting up manual thresholds for monitored devices.
- The system must support the ability to create reports that allow the surveillance administrators to search all IP traffic over a specified historical period, for a variety of conditions for critic al router interfaces
- The proposed system must be capable of providing the following detailed analysis across surveillance domain:
    - Top utilized links (inbound and outbound) based on utilization of link
    - Top protocols by volume based on utilization of link
    - Top host by volume based on utilization of link

- **Centralized Helpdesk System**
    - The proposed Helpdesk solution must provide flexibility of logging, viewing, updating and c losing incident manually via web interface for issues related to surveillance project.
    - Helpdesk system should provide incident management, problem management templates along with Helpdesk SLA system for tracking SLA's pertaining to incident resolution time for priority / non-priority incidents.
    - The proposed Helpdesk solution must have a built-in workflow engine to define escalations or tasks to be carried out after issues or change order are logged pertaining to surveillance project.
    - Centralized Helpdesk System should have integration with Network / Server Monitoring Systems so that the Helpdesk Operators can associate alarms with Service Desk tickets to help surveillance operators that for what alarms corresponding helpdesk tickets get logged.
    - Surveillance Network admin should be able to manually create tickets through Fault Management GUI. System should also automatically create tickets based on alarm type. System should provide a link to directly launch a Service Desk view of a particular ticket created by alarm from within the Network Operation console.

9. Directory services

- Should be compliant with LDAP v3, Support for integrated LDAP compliant directory services to record information for users and system resources, should provide integrated authentication mechanism across operating system, messaging service es, should provide directory services for ease of management and administration /replication, should provide support for Group Policies and software restriction Policies, should support security features, such as Kerberos, Smart Cards, Public Key Infrastructure (PKI), etc.
- Should provide support for X.500 naming standards, should support Kerberos for logon and authentication, should support that password reset capabilities for a given group or groups of users can be delegated to any nominated user.
- Should support that user account creation/deletion rights within a group or groups can be delegated to any nominated user.
- Should support directory services integrated DNS zones for ease of management and administration/replication.

10. Edge Level Switch (at Camera locations)

#	Parameter	Minimum Specifications
1.	Type	Managed Outdoor Industrial grade switch
2.	Total Ports	• Minimum 4 10/100 TX PoE • May require higher port density at some locations, depending upon site conditions • May require fiber ports at some locations, depending upon site conditions/distances.
3.	PoE Standard	IEEE 802.3af or better
4.	Protocols	• Support 802.1Q VLAN • DHCP support • SNMP Management
5.	Access Control	• Support port security • Support 802.1x (Port based network access control). • Support for MAC filtering.
6.	PoE Power per port	Sufficient to operate the CCTV cameras connected
7.	Rating	IP 31 or equivalent Industrial Grade Rating
8.	Operating Temperature	0 - 50 C or better

11. Data Center/server room / Aggregation Switches (Manageable)

#	Parameter	Minimum Specifications
1.	Ports	24 or 48 (as per requirements) 10/100/1000 Base-TX Ethernet ports and extra 2 no's of Base-SX/LX ports All ports can auto-negotiate between 10Mbps/ 100Mbps/ 1000Mbps, half-duplex or full duplex and flow control for half- duplex ports.
2.	Switch type	Layer 3
3.	MAC	Support 8K MAC address.
4.	Backplane	56 Gbps or more Switching fabric capacity
5.	Forwarding rate	Packet Forwarding Rate should be 70.0 Mpps or better
6.	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks
7.	Flow Control	Support IEEE 802.3x flow control for full-duplex mode ports.
8.	Protocols	Support 802.1D, 802.1S, 802.1w, Rate limiting Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping 802.1p Priority Queues, port mirroring, DiffServ Support based on 802.1p priority bits with at least 8 queues DHCP support & DHCP snooping/relay/optional 82/ server support Shaped Round Robin (SRR) or WRR scheduling support. Support for Strict priority queuing & Sflow Support for IPV6 ready features with dual stack Support up to 255 VLANs and up to 4K VLAN IDs
9.	Access Control	Support port security Support 802.1x (Port based network access control). Support for MAC filtering. Should support TACACS+ and RADIUS authentication

10.	VLAN	Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN The switch must support dynamic VLAN Registration or equivalent Dynamic Trunking protocol or equivalent
11.	Protocol and Traffic	Network Time Protocol or equivalent implementation Network Time Protocol support Switch should support traffic seg Traffic classification should be based on user- definable application types: TOS, DSCP, Port based, TCP/UDP port number
12.	Management	Switch needs to have RS-232 console port for management via console terminal or PC Must have support SNMP v1, v2 and v3 Should support 4 groups of RMON Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP etc. Configuration management through CLI, GUI based software utility and using web interface

12.KVM Module

#	Item	Minimum Specifications
1.	KVM Requirement	Keyboard, Video Display Unit and Mouse Unit (KVM) for the IT Infrastructure Management at Data Center
2.	Form Factor	19" rack mountable
3.	Ports	minimum 8 ports
4.	Server	It should support both USB and PS/2 connections.
	Connections	
5.	Auto-Scan	It should be capable to auto scan servers
6.	Rack Access	It should support local user port for rack access
7.	SNMP	The KVM switch should be SNMP enabled. It should be operable from remote locations
8.	OS Support	It should support multiple operating system
9.	Power Supply	It should have dual power with failover and built-in surge protection
10.	Multi-User support	It should support multi-user access and collaboration

13.First Level Router (Edge Level)

#	Item	Minimum Specifications
1.	Ports	The router should have 2 LAN & 2 WAN slots loaded with minimum one 2-port sync/async Serial Interface card and cable for connectivity to Internet / other offices. The sync / async port should support data rates of up-to 128Kbps in sync mode
2.	Speed	As per requirement
3.	Protocol Support	Must have support for TCP/IP, PPP, X.25, Frame relay and HDLC, must support VPN, must have support for integration of data and voice services Routing protocols of RIP, OSPF, and BGP.
4.	SNMP	Must be SNMP manageable

14. Second Level (Aggregation) Level Routers

#	Item	Minimum Specifications
1.	Ports	The router should have 2 LAN & 5 WAN slots loaded with minimum one 4- port sync/async Serial Interface card or 4- port channelized E1 card with cable for connectivity to Internet / other offices. The sync / async port should support data rates of up-to 128Kbps in sync mode
2.	Speed	As per requirement
3.	Protocol Support	Must have support for TCP/IP, PPP, X.25, Frame relay and HDLC, must support VPN. Must have support for integration of data and voice services Routing protocols of RIP, OSPF, and BGP. Support IPV4 & IPV6
4.	Manageability	Must be SNMP manageable
5.	Multi-Services	Should deliver multiple IP service es over a flexible combination of interfaces
6.	Scalable	The router should be scalable. For each slot multiple modules should be available
7.	Traffic control	Traffic Control and Filtering features for flexible user control Policies
8.	Bandwidth	Bandwidth on demand for cost effective connection performance enhancement
9.	Remote Access	Remote access features
10.	Redundancy	Redundancy in terms of Power supply
11.	Security features	MD5 encryption for routing protocol NAT URL based Filtering RADIUS Authentication Management Access Policy IPsec / Encryption
12.	QOS Features	RSVP, Priority Queuing, Policy based routing Traffic shaping, Time-based QoS Policy Bandwidth Reservation / Committed Information Rate

15. Central (Core) Router

#	Item	Minimum Specifications
1.	Multi-Services	Should deliver multiple IP services over a flexible combination of interfaces.
2.	Ports	As per overall network architecture proposed by the bidder, the router should be populated with required number of LAN/WAN ports/modules, with cable for connectivity to other network elements.

3.	Speed	As per requirement, to cater to entire bandwidth requirement of the project.
4.	Interface modules	Must support up to 10G interfaces. Must have capability to interface with variety interfaces.
5.	Protocol Support	Must have support for TCP/IP, PPP, X.25, Frame relay and HDLC Must support VPN. Must have support for integration of data and voice services. Routing protocols of RIP, OSPF, and BGP. Support IPV4 & IPV6.
6.	Manageability	Must be SNMP manageable.
7.	Scalable	The router should be scalable. For each slot multiple
		modules should be available. The chassis offered must have free slots to meet the scalability requirement of expansion of the project in the future.
8.	Traffic control	Traffic Control and Filtering features for flexible user control Policies.
9.	Bandwidth	Bandwidth on demand for cost effective connection performance enhancement
10.	Remote Access	Remote access features
11.	Redundancy	Redundancy in terms of Power supply(s). Power supply should be able to support fully loaded chassis All interface modules, power supplies should be hot-swappable
12.	Security features	MD5 encryption for routing protocol NAT, URL based Filtering, RADIUS Authentication Management Access Policy, IPsec / Encryption L2TP
13.	QOS Features	RSVP, Priority Queuing, Policy based routing Traffic shaping, Time-based QoS Policy Bandwidth Reservation / Committed Information Rate

16. Firewall

#	Item	Minimum Specifications
1.	Physic al attributes	Should be mountable on 19” Rack Internal redundant power supply
2.	Interfaces	8 x GE, upgradable to 16 GE Console Port 1 number

3.	Performance and Availability	Encrypted throughput: minimum 800 Mbps Concurrent connections: up to 100,000 Simultaneous VPN tunnels: 2000
4.	Routing Protocols	Static Routes RIPv1, RIPv2 OSPF
5.	Protocols	TCP/IP, PPTP RTP, L2TP
		IPsec, GRE, DES/3DES/AES PPPoE, EAP-TLS, RTP FTP, HTTP, HTTPS SNMP, SMTP DHCP, DNS Support for IPv6
6.	Other support	802.1Q, NAT, PAT, IP Multicast support, Remote Access VPN, Time based Access control lists, URL Filtering, support VLAN, Radius/ TACACS
7.	QoS	QoS features like traffic prioritization, differentiated services, committed access rate. Should support for QoS features for defining the QoS Policies.
8.	Management	Console, Telnet, SSHv2, Browser based configuration SNMPv1, SNMPv2

17. Intrusion Prevention System

#	Item	Required Specifications
1.	Performance	Should have an aggregate throughput of no less than 200Mbps Total Simultaneous Sessions – 500,000
2.	Features	IPS should have Dual Power Supply. IPS system should be transparent to network, not default gateway to Network. IPS system should have Separate interface for secure management. IPS system should be able to protect Multi Segment in the network, should be able to protect 4 segments.
3.	Real Time Protection	Web Protection, Mail Server Protection Cross Site Scripting, SNMP Vulnerability Worms and Viruses, Brute Force Protection SQL Injection, Backdoor and Trojans
4.	Stateful Operation	TCP Reassembly IP Defrag Bi- directional Inspection Forensic Data Collection Access Lists

5.	Signature Detection	Should have provision for Real Time Updates of Signatures, IPS Should support Automatic signature synchronization from database server on web Device should have capability to define User Defined Signatures
6.	Block attacks in real time	Drop Attack Packets Reset Connections Packet Logging Action per Attack
7.	Alerts	Alerting SNMP Log File Syslog E- mail
8.	Management	SNMP V1, 2C, 3 HTTP, HTTPS SSH, Telnet, Console
9.	Security Maintenance	IPS Should support 24/7 Security Update Service IPS Should support Real Time signature update IPS Should support Provision to add static own attack signatures System should show real-time and History reports of Bandwidth usage per Policy IPS should have provision for external bypass Switch

18. VSAT (Optional/on need basis or as per requirement of user dept)

#	Parameter	Minimum Specifications
1.	VSAT	• Ku-Band • Should be fully controlled from the central NMS • Should Support DVB- S2, RIP V1, RIP V2, IGMP, IP Multicast. • The VSAT should have a single compact enclosure supporting LAN interface. • The VSAT must have uplink data rate of minimum 2Mbps • Automatic satellite acquisition and tracking • Low profile antennae • SLA for VSAT connectivity Latency shall be at 1 Sec (from Mobile Van to the Command Centre)

DG

Sr No	Item	Specifications
1	General Specifications	Auto Starting DG Set mounted on a common base frame with AVM (Anti-Vibration) pads, residential silencer with exhaust piping, complete conforming to ISO 8528 specifications and CPCB certified for emissions. KVA rating as per the requirement
2	Engine	Radiator cooled, multi cylinder, 1500 RPM diesel engine, with electronic/manual governor and electric al starting arrangement complete with battery, conforming to BS 5514/ ISO 3046/ IS 10002
3	Fuel	High Speed Diesel (HSD)

5	Alternator	Self-exciting, self-regulating type alternator rated at 0.8 PF or better, 415 Volts, 3 Phase, 4 wires, 50 cycles/sec, 1500 RPM, conforming to IS 4722/ BS 5000, Windings of 100% Copper, c lass H insulation, Protection as per IP 23.
6	AMF (Auto Main	AMF Panel fitted inside the enclosure, with the following:
	Failure) Panel	It should have the following meters/indicators Incoming and outgoing voltage Current in all phases Frequency KVA and power factor Time indication for hours/minutes of operation Fuel Level in fuel tank, low fuel indication Emergency Stop button Auto/Manual/Test selector switch MCCB/Circuit breaker for short-circuit and overload protection Control Fuses Earth Terminal Any other switch, instrument, relay etc. essential for Automatic functioning of DG set with AMF panel
7	Acoustic Enclosure	The DG set shall be provided with acoustic enclosure / canopy to reduce the sound level and to house the entire DG set (Engine & Alternator set) assembly outside (Open- air). The enclosure must be weather resistant powder coated, with insulation designed to meet latest MOEF/CPCB norms for DG sets, capable to withstand City climate. The enclosure must have ventilation system, doors for easy access for maintenance, secure locking arrangement, complete and
8	Fuel Tank Capacity	It should be sufficient and suitable for containing fuel for 12 hours continuous operation, Complete with level indicator, fuel inlet and outlet, air vent, drain plug, inlet arrangement for direct filling and set of fuel hoses for inlet and return.

4. SLA

Sr. No.	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Point	Metric	Points	Metric	Points
1. Camera, Video Feed Uptime and Quality							
1	Uptime per camera (live feed available irrespective of network/power/etc. issues)	98%	10	>= 96% to <98%	5	< 96%	0
2	Ratio of Live cameras v/s Total number of cameras at any point of time (To be measured every 1	97%	5	>= 93% to <97 %	2.5	< 93%	0

	hour) #						
3	At CP Office command Centre: Live camera feed available from selected cameras for viewing) at any given time	98%	4	>= 96% to <98%	2	< 96%	0
4	At 2nd Command Center Centre : Live camera feed available from selected cameras for viewing) at any given time	98%	2	>= 96% to <98%	1	< 96%	0
5	At Regional & Zonal Office Viewing Centers: Live camera feed available from respective region's cameras at any given time	98%	5	>= 96% to <98%	2.5	< 96%	0
6	At Police Stations: Live camera feed available from respective Police station jurisdiction cameras at any given time	97%	7	>= 94% to <97%	3.5	< 94%	0

-

Sr. No.	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Point	Metric	Points	Metric	Points
1. Camera, Video Feed Uptime and Quality							
1	Uptime per camera (live feed available irrespective of network/power/etc. issues)	98%	10	>= 96% to <98%	5	< 96%	0
2	Ratio of Live cameras v/s Total number of cameras at any point of time (To be measured every 1 hour) #	97%	5	>= 93% to <97 %	2.5	< 93%	0
3	At CP Office command Centre: Live camera feed available from selected cameras for viewing) at any given time	98%	4	>= 96% to <98%	2	< 96%	0
4	At 2nd Command Center Centre : Live camera feed available from selected cameras for viewing) at any given time	98%	2	>= 96% to <98%	1	< 96%	0
5	At Regional & Zonal Office Viewing Centers: Live camera feed available from respective region's cameras at any given	98%	5	>= 96% to <98%	2.5	< 96%	0

	time						
6	At Police Stations: Live camera feed available from respective Police station jurisdiction cameras at any given time	97%	7	>= 94% to <97%	3.5	< 94%	0

-

Sr. No.	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Point	Metric	Points	Metric	Points
b.	At Regional & Zonal Viewing Centers & Police Stations	< 4 sec	0.5	4.01 - 7.0 secs	0.25	>7 secs	0
4	Menu Navigation, Window/Screen Opening, Screen Navigation (Average)						
a.	At Main Control Room, 2nd Command Center & Traffic Control Center	<2 sec	0.5	2.01 - 5.0 secs	0.25	>5 secs	0
b.	At Regional & Zonal Viewing Centers & Police Stations	<4 secs	0.5	4.01 - 7.0 secs	0.25	>6 secs	0
5	Change of Screen from one camera Source to another						
a.	At Main Control Room, 2nd Command Center & Traffic Control Center	<2 sec	0.5	2.01 - 6.0 secs	0.25	>6 secs	0
b.	At Regional & Zonal Viewing Centers & Police Stations	<4 secs	0.5	4.01 - 7.0 secs	0.25	>7 secs	0
6	Video Feed Query Retrieval Response Time	Implementation query - <5secs Medium complexity query - < 10 secs High Complexity query - < 15secs	1	Implementation Complexity Query: 5.01-10 secs Medium Complexity Query: 10.01-15 secs High Complexity Query: 15.01-20 secs	0.5	Implementation Complexity Query: > 10 secs Medium Complexity Query: > 15 secs High Complexity Query: > 20 secs	0
7	Reports Generation Response Time (Alerts/MIS/Logs etc.)	Implementation query - < 5secs Medium complexity query - <30 secs High Complexity query - < 1min	1	Implementation complexity Query = 5.01 - 10 secs Medium complexity query = 30.01 - 60 secs High Complexity query = < 60.1 sec - 2 min	0.5	Implementation complexity Query = > 10 secs Medium complexity query = > 60 secs High Complexity query = > 2 min	0
8	PTZ Lag time (movement at	< 2 sec	1	2.01 - 4.0 secs	0.5	>4 secs	0

-

Sr. No.	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Point	Metric	Points	Metric	Points
	keyboard/joystick and actual moving indication through video feed viewed						
9	Maximum time for successful camera settings modification	< 4 secs	0.5	4.01 - 6.0 secs	0.25	>6 secs	0
3. Video Analytics Performance							
1	ANPR for Standard Roman Number plates (3 wheelers & above)	80%	1	79.99% to 70%	0.5	< 70 %	0
2	ANPR for Non-Standard Roman Number plates (3 wheelers & above)	50%	0.5	49.99% to 40%	0.25	< 40 %	0
3	ANPR for Standard Roman Number plates (2 wheelers)	70%	0.3	69.99% to 60%	0.15	< 60 %	0
4	ANPR for Non-Standard Roman Number plates (2 wheelers)	50%	0.2	49.99% to 40%	0.1	< 40%	0
5	Any other analytics (SLA to be defined in discussion with successful bidder)	80%	1	79.99% to 70%	0.5	< 70%	0
4. Mobile Van and GPS-Enabled vehicles							
1	VSAT Link uptime for the mobile Vans, Data Centers & Command Centers	99.50%	2	>= 97 % to <99.5%	1	< 97 %	0
2	Uptime of GPS-trac ked vehicles / Vans at central command center (in GIS application) including uptime of GPS-tracking unit	99.50%	2	>= 97 % to <99.5%	1	< 97 %	0
3	Availability (road worthiness) of	99.50%	1	>= 97 % to <99.5%	0.5	< 97 %	0

-

Sr. No.	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Point	Metric	Points	Metric	Points
	the Mobile Vans						
5. End-User Equipment Uptime							
1	Monitoring workstations at Command Centers	99 %	2	>= 96 % to <99%	1	< 96 %	0
2	Video walls	99%	1	>= 96 % to <99%	0.5	< 96 %	0
3	IP Phones	98%	1	>= 96 % to <98%	0.5	< 96 %	0
4	Monitoring workstations at Viewing Stations and mobile Vans	95%	1	>= 90 % to <95 %	0.5	< 90 %	0

5	TV screens at Zonal Offices, Police stations and mobile Vans	95%	1	>= 90 % to <95 %	0.5	< 90 %	0
6. Underlying IT Infrastructure Uptime/Availability at Data Centers							
1	Production Servers Uptime	99.95%	4	>= 99.5 % to <99.94%	2	< 99.5%	0
2	Storage System Uptime	99.95%	3	>= 99.5 % to <99.94%	1.5	< 99.5%	0
3	Fire detection and suppression system uptime	100%	1	>=99.95% to 100%	0.5	<99.95%	0
4	Physic al Security	Fully compliant	1	Lacunae shown in compliance procedures	0.5	For every Non-compliance instance	0
5	CCTV surveillance of data centre area	100%	1	98%-100%	0.5	< 98%	0
7. Security /Patch Services for IT Infrastructure							
1	Firewall and any other security appliance Uptime	100%	1	97 % to 99.99%	0.5	< 97%	0

-
-

Sr. No.	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Point	Metric	Points	Metric	Points
2	Security rules update within 2 hours of approved change management request	0 violations of service parameters	0.5	1 – 4 violations	0.25	> 4 violations	0
3	Anti-virus, Anti-spyware, Anti-spam updates within 24 hrs. of request	0 violations of service parameters	0.5	1 – 4 violations	0.25	> 4 violations	0
4	Critic al Patches – within 48 hours of patch release.	0 violations of service parameters	0.5	1 – 4 violations	0.25	> 4 violations	0
5	Non-Critical Patches - within 15 days of patch release.	Up to 1 violations of service parameters	0.5	2 – 5 violations	0.25	> 5 violations	0
8. Technical Helpdesk, Trouble Ticketing, Issue Resolution							
1	Average Speed of Answer	<= 10 secs	0.5	10 to 14 secs	0.25	> 14 sec	0
2	Average Call Lost Rate	0 – 0.1	1	0.1 - 2.00%	0.5	> 2 %	0
3	Resolution of Critical Issue (that impacts more than one production services & higher mgmt. call)	60 minutes	1.5	60.01 to 75 min	0.75	> 75 min	0
4	Resolution of Medium Level Issue (that does not impact production services)	120 minutes	1	120.01 to 240 min	0.5	> 240 min	0

5	Resolution of low-level Issue (upgrade, shifting and preventive maintenance (of non-production items))	2 days	1	>2 to 3 days	0.5	> 3 days	0
	Total Score		100		50		0

5. Access Control of command center /viewing center Camera feed and data on media

Access Control of command center /viewing center Camera feed and data on media
1. Formation of Access Control Management Unit 2. SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS 3. POLICIES & PROCEDURES RELATING TO RETENTION, ACCESS & USE OF THE DATA 4. POLICIES & PROCEDURES RELATING TO PUBLIC ACCESS OR USE OF THE DATA 5. INTERNAL AUDIT & OVERSIGHT MECHANISMS

6. Drones and Unmanned Vehicles details

Drones and Unmanned Vehicles details	Unmanned aerial vehicles (UAV) and Drones are going to be critical components in future to any security surveillance system where these machines can be deployed into sensitive / inhospitable environments for surveillance and transmitting video feeds to the Command center. Integration with Third party drones as an option could also be explored.

7. Proposed Eligibility Criteria

For Metro Location and State Capital (cameras more than 5000)	1. The bidder (or all consortium partners) must be a registered company in India, registered under the Companies Act 1956. The bidder should be operating in India for the last five years as on 31/03/2023 or end of current financial year whichever is applicable. 2. The bidder (prime bidder in case of consortium) should have overall revenue (gross income) of minimum **Rs. 1000 Cr from IT/ITES/Telecom or Public Infrastructure Projects** in each of the last **3 financial years** as on 31/03/2023 (based on CVC guidelines).

	• In case of consortium, each consortium partner should have over revenue (gross income) of minimum **Rs. 500 Cr from IT/ITES/Telecom or Public Infrastructure Projects** in each of the last **3 financial years** as on 31/03/2023 (based on CVC guidelines). • In case of consortium, **maximum number of consortium partners allowed shall be three**. Consortium partners shall sign a consortium agreement format given in the RFP. 3. The bidder (or all consortium partners) should have a **positive net worth** as on 31/03/2023. 4. The bidder (prime bidder in case of consortium) should have made cumulative net profit of minimum **Rs. 500 Crores** in the last **5 Financial Years** as on 31/03/2023. 5. The bidder (prime bidder in case of consortium) should have a valid ISO 9001:2008 or should an SEI CMM Level 3 (or above) certification. 6. The bidder (or all consortium partners) should submit valid documentary proof of Sales Tax/VAT registration number and the details of income tax registration (PAN).
<u>For Non-Metro other than state capital (Camera up to 1000)</u>	1. The bidder (or all consortium partners) must be a registered company in India, registered under the Companies Act 1956. The bidder should be operating in India for the last five years as on 31/03/2023. 2. The bidder (prime bidder in case of consortium) should have overall revenue (gross income) of minimum **Rs. 250 Cr from IT/ITES/Telecom or Public Infrastructure Projects** in each of the last **3 financial years** as on 31/03/2023(based on CVC guidelines). • In case of consortium, each consortium partner should have over revenue (gross income) of minimum **Rs. 100 Cr from IT/ITES/Telecom or Public Infrastructure Projects** in each of the last **3 financial years** as on 31/03/2023(based on CVC guidelines). • In case of consortium, **maximum number of consortium partners allowed shall be three**. Consortium partners shall sign a consortium agreement format given in the RFP. 3. The bidder (or all consortium partners) should have a **positive net worth** as on 31/03/2023. 4. The bidder (prime bidder in case of consortium) should have made cumulative net profit of minimum **Rs. 100 Crores** in the last

	5 Financial Years as on 31/03/2023. 5. The bidder (prime bidder in case of consortium) should have a valid ISO 9001:2008 or should an SEI CMM Level 3 (or above) certification. 6. The bidder (or all consortium partners) should submit valid documentary proof of Sales Tax/VAT registration number and the details of income tax registration (PAN). **Notes:** a) In case of Central Govt./PSU in IT/ITES/Telecom business or Public Infrastructure Projects, criteria **2)** will be applicable and criteria **3)** and **4)** can be relaxed b) In case of consortium, a consortium partner shall only participate in one consortium bid unless the partner is an OEM or Network Service Provider and has been part of consortium only as OEM or Network Service Provider.
<u>For Non-Metro other than state capital (Camera up to 250)</u>	1. The bidder (or all consortium partners) must be a registered company in India, registered under the Companies Act 1956. The bidder should be operating in India for the last five years as on 31/03/2023. 2. The bidder (prime bidder in case of consortium) should have overall revenue (gross income) of minimum **Rs. 100 Cr from IT/ITES/Telecom or Public Infrastructure Projects** in each of the last **3 financial years** as on 31/03/2023 (based on CVC guidelines). • In case of consortium, each consortium partner should have over revenue (gross income) of minimum **Rs. 50 Cr from IT/ITES/Telecom or Public Infrastructure Projects** in each of the last **3 financial years** as on 31/03/2023(based on CVC guidelines). • In case of consortium, **maximum number of consortium partners allowed shall be three**. Consortium partners shall sign a consortium agreement format given in the RFP. 3. The bidder (or all consortium partners) should have a **positive net worth** as on 31/03/2023. 4. The bidder (prime bidder in case of consortium) should have made cumulative net profit of minimum **Rs. 50 Crores** in the last **5 Financial Years** as on 31/03/2023. 5. The bidder (prime bidder in case of consortium) should have a valid ISO 9001:2008 or should an SEI CMM Level 3 (or above) certification. 6. The bidder (or all consortium partners) should submit valid

	documentary proof of Sales Tax/VAT registration number and the details of income tax registration (PAN). **Notes:** c) In case of Central Govt./PSU in IT/ITES/Telecom business or Public Infrastructure Projects, criteria **2)** will be applicable and criteria **3)** and **4)** can be relaxed 7. In case of consortium, a consortium partner shall only participate in one consortium bid unless the partner is an OEM or Network Service Provider and has been part of consortium only as OEM or Network Service Provider
<u>For Non-Metro other than state capital (Camera up to 100)</u>	1. The bidder (or all consortium partners) must be a registered company in India, registered under the Companies Act 1956. The bidder should be operating in India for the last five years as on 31/03/2023. 2. The bidder (prime bidder in case of consortium) should have overall revenue (gross income) of minimum **Rs. 20 Cr from IT/ITES/Telecom or Public Infrastructure Projects** in each of the last **3 financial years** as on 31/03/2023(based on CVC guidelines). • In case of consortium, each consortium partner should have over revenue (gross income) of minimum **Rs. 10 Cr from IT/ITES/Telecom or Public Infrastructure Projects** in each of the last **3 financial years** as on 31/03/2023 (based on CVC guidelines). • In case of consortium, **maximum number of consortium partners allowed shall be three**. Consortium partners shall sign a consortium agreement format given in the RFP. 3. The bidder (or all consortium partners) should have a **positive net worth** as on 31/03/2023. 4. The bidder (prime bidder in case of consortium) should have made cumulative net profit of minimum **Rs. 10 Crores** in the last **5 Financial Years** as on 31/03/2023. 5. The bidder (prime bidder in case of consortium) should have a valid ISO 9001:2008 or should an SEI CMM Level 3 (or above) certification. 6. The bidder (or all consortium partners) should submit valid documentary proof of Sales Tax/VAT registration number and the details of income tax registration (PAN). **Notes:** d) In case of Central Govt./PSU in IT/ITES/Telecom business or Public Infrastructure Projects, criteria **2)** will be applicable

	and criteria **3)** and **4)** can be relaxed 7. In case of consortium, a consortium partner shall only participate in one consortium bid unless the partner is an OEM or Network Service Provider and has been part of consortium only as OEM or Network Service Provider
Components for 100 camera surveillance system	1. **No datacenter component required can be done on DVR/NVR** 2. **SI to ensure security of data and viewing center** 3. **Camera as per assessment report of user department** 4. **DR may be taken on cloud only if option of High availability exhausted at local level** 5. **Timeline for implementation is within 3 months (Go Live)** 6. **Software and application to be part of the camera bundle (ANPR camera and its software)**

1. The bidder (or all consortium partners) must be a registered company in India, registered under the Companies Act 1956. The bidder should be operating in India for the last five years as on 31/03/2023 or end of current financial year whichever is applicable.

2. The bidder (prime bidder in case of consortium) should have average revenue (gross income) of minimum ***<<20 times the annual value of the project>>*** **from IT/ITES/Telecom or Public Infrastructure Projects** in the last **3 financial years** as on 31/03/2023.

   • In case of consortium, each consortium partner should have average revenue (gross income) of minimum ***<<5 times the annual value of the project>>*** **from IT/ITES/Telecom or Public Infrastructure Projects** in the last **3 financial years** as on 31/03/2023.

3. The bidder (or all consortium partners) should have a **positive net-worth** as on 31/03/2023.

4. The bidder (or any consortium partner) should have a valid ISO 9001:2008 certification

5. The bidder (or any consortium partner) should have a valid ISO 27001:2013 certification

6. The bidder (or all consortium partners) should submit valid documentary proof of GST and the details of income tax registration (PAN).

7. The Bidder (or ALL Consortium partners) should submit an affidavit that currently they are NOT under blacklisting by any of the Government Institutions in India.

8. Technical Evaluation Criteria

The Technical Evaluation Criteria will award marks based on the experience and competence of the bidder and the strength of the solution proposed. The evaluation would be carried out on 4 broad parameters as below:

- Technical Features - 45%
- Presentation - 10%

- Competence of the Bidder/Consortium - 35%
- Strength of Resources proposed - 10%

Parameter	Criteria	Max Marks
Technical Features	Compliance to the Detailed Specifications provided in the Scope of Work	10 marks
Technical Features	Standing in the IDC / Gartner / Forrester Report	10 marks
Technical Features	Reliability and Redundancy of the Architecture to ensure that the recording, storage, and viewing are error free - end to end. This should be conveyed in the proposal to be submitted	10 marks
Technical Features	Reliability and Redundancy of the Hardware to ensure that the recording, storage, and viewing are error free - end to end. This should be conveyed in the proposal to be submitted	10 marks
Technical Features	Capability of the Analytical Software - This should be conveyed in the proposal to be submitted	5 marks
Presentation	Presentation covering - Understanding of requirement, Solution proposed, Proof of concept for capability of Analytical software & Risk Management	10 marks
Competence of the Bidder/Consortium	Overall Turnover of the Lead Bidder <<Depending on the value provided in the PQ, step up by 10% for each 2 marks>>	10 marks
Competence of the Bidder/Consortium	Number of projects executed for any Government Institution in India with a value of more than <<estimated value of this project>> Crores: 2 Project - 2 marks 4 Projects - 4 marks 6 Projects - 6 marks 8 Projects - 8 marks 10 Projects - 10 marks 12 Projects - 12 marks 15 Projects - 15 marks	15 marks
Competence of the Bidder/Consortium	Number of International projects executed with a value of more than <<half the estimated value of this project>> Crores: 2 Project - 2 marks 4 Projects - 4 marks 6 Projects - 6 marks 8 Projects - 8 marks 10 Projects - 10 marks	10 marks
Resources proposed	Strength of Resources proposed - Resources will be evaluated based on number of projects, number of international projects and Domain experience (Surveillance domain) elaborated in the Resume	10 marks

9. Commercial Bid Format

Summary of all Cost Components

Sr.No	Item	Ref. Schedule	Total Price
CAPITAL COST			
1.	Edge Devices	A	
2.	Data Center 1-Primary data Center (DC)/ Server Room	B	
3.	Data Center 2 – Secondary Data center (DR)/Server Room	B	
4.	Integrated Central Command Center	C	
5.	2nd Command Center	C	
6.	State Viewing Center	C	
7.	Regional Office Viewing Centers	C	
8.	Police Stations	C	
9.	DCP/SP Office Infrastructure	C	
10.	Infrastructure at Mantralaya for viewing of feeds (need basis)	C	
11.	Infrastructure at project HQ for viewing of feeds (Need Basis)	C	
12.	Mobile apps for viewing feeds	D	
13.	Picture Intelligence Unit	C	
14.	Miscellaneous Costs	E	
(I) CAPEX			
OPERATIONAL COST FOR 5 YEARS			
15.	Bandwidth Cost	o	
16.	Electricity Cost	p	
17.	Operations & Maintenance for IT/non IT Infrastructure	q	
18.	Managed Hosting Costs	r	
19.	Incremental Unit Costs	u	
20.	Support Cost for Picture Intelligence Unit		
21.	Costs to connect other establishments for Collaborative monitoring		
22.	Miscellaneous Costs		
(II) OPEX for 5 Years			
Grand Total (I+II)			
Grand Total in Words			

10. Ref.Schedule

Schedule A – Edge Devices

Sr.No	Description	Qty.	UnitRate (INR)	Total Amount (INR) – A	Taxes & Duties (INR) – B	Total (INR) – A+B
1.	Outdoor Box Cameras *	Actual (please specify)				

2.	Outdoor PTZ Cameras	Actual (please specify)				
3.	IR Illuminators	Actual (please specify)				
4.	Thermal Cameras	Actual (please specify)				
5.	Poles for Cameras andEquipment's	Actual (please specify)				
6.	Provisioning of Electrical Power	Actual (please specify)				
7.	Switches	Actual Qty arrived for the solution (please specify)				
8.	Routers					
9.	Networking Cost (Passive Components) (Pl. specify the details like Junction Box Patch Panel LIU OFC CAT 6 cable Patch cords Pipes Media Converters Installation and Labor costs					
10.	Physical labor for digging, refilling, RI, etc.					
11.	Any other Cost (Pl. specify)					
12.	Road Re-Instatement,Row, etc.					
13.	<Any other cost element>					
Total for Schedule A						

Schedule B – Data Center 1 & 2

Sr.No	Description	Qty.	UnitRate (INR)	Total Amount (INR) - A	Taxes &Duties (INR) - B	Total (INR) = A+B
1	Servers (inclusive of Operating System)					
1.a	Application Servers					
1.b	Recording Server					
1.c	Analytics Server					
1.d	Database Server					
1.e	Management Server					
1.f	Enterprise Backup Server					

1.g	Domain Controller					
1.h	Any other Server required tocater to the scope of work mentioned					
2	Application & System Software					
2.a	Video Management System including Customized Mobile Application to integrate smartphones / tablets for 2-way communication					
2.b	Software for Recording, Viewing of Videos					
2.c	Updated Base Map of City (min. 0.6 mtr resolution, min. 1:500)					
2.e	RDBMS (if required)					
2.f	Backup Solution					
2.g	Enterprise Management System (Give breakup for SLAMgmt., Helpdesk Mgmt., Network Mgmt., BMS, etc. if applicable)					
2.h	Anti-virus Software					
2.i	LDAP Software					
2.j	Customized Software Dashboard for Police Department (for various levels)					
2.k	Any other Server-side Software required to caterto the scope of work mentioned					
3	Primary Storage	As per estimation done in solution proposed				
4	Secondary Storage					
5	Storage ManagementSystem					
6	Tape Library					
7	Core Router					
8	Switches					
8.1	L2 Switches					
8.2	L3 Switches					
9	KVM Switches					
10	Firewall					

11	Intrusion Prevention System					
12	Racks (Caged)					
13	Fireproof Enclosure for Media Storage					
14	Networking Cost (Passive Components) (Pl. specify the details)					
15	Any Other Component(s) to Cater to the requirements of Scope of Work mentioned in Vol II					
Total for Schedule B						

Schedule C – CP/SP Office Command Center/Viewing centers

Sr.No	Description	Qty.	UnitRate (INR)	Total Amount (INR) – A	Taxes & Duties (INR) - B	Total (INR) – A+B
1.	Video Wall (along with hardware & software) (8(4x2) cubes)	Pl specify				
2.	Monitoring Workstations	Pl specify				
3.	Switches	Pl specify				
4.	Router	1				
5.	Networking/IT Racks	Pl specify				
6.	Networking Cost (Passive Components) (Pl. specifythe details)	Pl specify				
7.	Electrical Cabling &Necessary Illumination Devices	Pl specify				
8.	Fire Safety System with alarms	Pl specify				
9.	Public Address System	Pl specify				
10.	Access Control System (RFID/Proximity based, forall staff)	Pl specify				
11.	UPS (30-minute backup)	1				
12.	DG Set	1				
Total for Schedule C						

Schedule D

Sr.No	Description	Qty.	UnitRate (INR)	Total Amount (INR) – A	Taxes & Duties (INR) - B	Total (INR) – A+B
1	Define the App Concept and Purpose					

2	Market Research and Competitive Analysis					
3	Create Wireframes and Prototypes					
4	Choose a Development Approach					
5	Select a Development Stack					
6	Develop the Backend (if required)					
7	Frontend Development					
8	App Testing and Quality Assurance					
9	User Feedback and Iteration					
10	Security and Privacy Considerations					
11	App Monetization Strategy					
12	App Store Submission					
13	Marketing and Promotion					
14	App Maintenance and Updates					
15	User Support and Feedback Management					
16	*Any other Additional Cost Components to cater to requirements of project*					
17	Total for Schedule D					

Schedule E – CP/SP Office Command Center/Viewing centers

Sr.No	Description	Qty.	UnitRate (INR)	Total Amount (INR) – A	Taxes & Duties (INR) - B	Total (INR) – A+B
1.	Training Costs (per batch)					
1.a	Functional Training	10 batches				
1.b	Administrative Training	1 batch				
2.c	Sr. Management Training	4 batches				
2.	Hardware, Software forsupporting creation of legal evidence on CDs / DVDs in an untamperedmanner	Pl specify				
3.	Desktop for HelpdeskExecutives	Pl Specify				
4.	Project Management Cost(Pre-Go Live Stage)	Pl Specify				
5.	*Any other Additional Cost Components to cater to requirements of project*					
Total for Schedule D						

Schedule O – Bandwidth Costs

Sr. No	Description	Qty.	Minimum Bandwidth (Pl specify) #	Unit Rate for Bandwidth proposed	Amount in Rs.				
					1st Year	2nd Year	3rd Year	4th Year	5th Year
1.	Bandwidth for Outdoor Box Cameras(Cameras – Data Center)	Pl Specify							
2.	Bandwidth for Outdoor PTZ Cameras (Cameras – Data Center)	Pl Specify							
3.	Bandwidth for Thermal Cameras (Cameras – Data Center)	Pl Specify							
4.	CP Office – Data Center	Pl Specify							
5.	2nd Command Center – Data Center	Pl Specify							
6.	Regional Viewing Center – Data Center	Pl Specify							
7.	Zonal Offices – Data Center	Pl Specify							
8.	Data Center 1- Data Center 2	Pl Specify							
9.	Policee Station – Data Center	Pl Specify							
Subtotal									
Total for Schedule O									

Schedule P – Electricity Costs

Sr. No	Description	Qty.	Amount in Rs.				
			1st Year	2nd Year	3rd Year	4th Year	5th Year
1.	Electricity charges at CP/SP Office ControlCentre	Pl Specify					
2.	Electricity charges at 2nd CommandControl Centre	Pl Specify					
3.	Electricity charges at Zonal/Police station viewing center	Pl Specify					
4.	Electricity Charges for Edge Devices						
Subtotal							
Total for Schedule P							

Schedule Q – Operations & Maintenance Costs for IT / Non-IT Infrastructure

Sr.No	Description	Qty.	Amount in Rs.				
			1st Year	2nd Year	3rd Year	4th Year	5th Year
1.	Edge Devices						
A	Outdoor Box Cameras	Pl Specify					
B	Outdoor PTZ Cameras	Pl Specify					
C	IR Illuminators	Pl Specify					
D	Thermal Cameras	Pl Specify					
E	Poles & Camera Accessories	Pl Specify					

F	Please add relevant subcomponents						
…							
2.	**Servers Side Infrastructure**						
A	Server1						
B	*Server 2*						
C	Storage Solution of 2 PT						
D	Firewall						
F	*Please add relevant subcomponents*						
G	Primary Storage						
H	Secondary Storage						
…							
3.	**Software**						
A	Video Management System						

B	*Other Software …*						
D	*Please add relevant subc o m p o n e n t s*						
….							
4.	**Client-Side Hardware**						
….	*Please add relevant subc o m p o n e n t s*						
7.	**Any other equipment**						
Sub-Total							
Total for **Schedule Q**							

Schedule R – Managed Hosting Costs

Sr. No	Description	Qty.	Amount in Rs.				
			1st Year	2nd Year	3rd Year	4th Year	5th Year
1.	Rack Space at Data Center 1 (DC1)						
2.	Seating Space for Project Team at DC1						
3.	Rack Space at Data Center 2 (DC2)						
4.	Seating Space for Project Team at DC2						
5.	*…. Please specify the relevant cost components*						
Subtotal							
Total for Schedule R							

Schedule U – Incremental Unit Costs

Sr. No	Description	Qty.(X)	Unit Rate in Rs. For each of the 5 years aftersuccessful Go Live					Total Cost [X * (A+B+C+D+E)]
			1st Year(A)	2nd Year (B)	3rd Year (C)	4th Year(D)	5th Year(E)	
1.	Outdoor Fixed Box Cameras	Each unit						
2.	Pan. Tilt and Zoom Cameras (PTZ)	Each unit						
3.	Thermal Cameras	Each unit						
4.	IR Illuminators	Each unit						
5.	Pole for Cameras (inclusive of junction boxes)	Each unit						
6.	Provisioning of Electrical Power	Each unit						
7.	Edge level Router/Switch (appropriate deviceas perthe original solution offered)	Each unit						
9.	Bandwidth Cost for connecting the New Camerato Data Center	Each unit						
10.	Networking Cost (Passive Components)	Each unit						

11.	Primary Storage	Each unit						
12.	Secondary Storage	Each unit						
13.	Workstation (with 3 Monitors)	Each unit						
14.	Workstation (with 1 Monitor)	Each unit						
15.	Any other Cost (Pl. specify)							
Total for Schedule U								

Schedule X – Costs to connect other establishments for collaborative monitoring

Sr. No	Description	Qty.	Total Cost in Rs.				
			1st Year	2nd Year	3rd Year	4th Year	5th Year
1.	Bandwidth cost for establishing 10 Mbps connection to one establishment(for 20 instances per year, each instance lasting for 2 days)	20 instances every year					
2.	Other Costs to provide the connectivity(Pl give details)						
Subtotal							
Total for Schedule X							

Schedule Z – Miscellaneous Costs

Sr. No	Description	Total Cost in Rs.				
		1st Year	2nd Year	3rd Year	4th Year	5th Year
1.	Please specify other relevant costs, not qualified inother sub-headings					
2.	…					
Total for Schedule Z						

11. Formula to estimate the number of cameras required per square kilometer of a city area.

This formula is a rough guideline and should be adjusted based on the specific characteristics and security needs of the city. The formula should consider factors such as population density, crime rates, and the objectives of the surveillance system. Here's a basic formula as a starting point

Number of Cameras per Square Kilometer = (C / A) x D

Where:

- **C** represents the estimated number of cameras needed for the entire city.
- **A** is the total area of the city in square kilometers.
- **D** is a density factor that can be adjusted based on specific factors, such as population density, crime rates, and the city's surveillance objectives.

The density factor (D) can be calculated as follows:

D = (PD x CR x SO) / 1000

Where:

- **PD** represents the population density in people per square kilometer.
- **CR** is the city's crime rate or security risk level, measured on a scale of 0 to 100 (higher values indicate higher crime rates or security risks).
- **SO** is a security objective factor, also measured on a scale of 0 to 100, reflecting the city's specific surveillance objectives (e.g., crime prevention, traffic monitoring, public safety).

Step-by-step process to use this formula:

1. Calculate the population density (PD) by dividing the city's population by its total area in square kilometers.
2. Determine the city's crime rate (CR) based on available crime statistics or security assessments. Convert the crime rate to a scale of 0 to 100.
3. Define the city's security objectives (SO) on a scale of 0 to 100, with higher values indicating a greater need for surveillance.
4. Calculate the density factor (D) using the formula.
5. Estimate the total number of cameras needed for the entire city (C) based on the city's size, security objectives, and the density factor (D).
6. Finally, calculate the number of cameras required per square kilometer using the formula.

This formula provides a starting point for estimating the number of cameras needed. It should be adjusted based on a detailed security assessment, specific city requirements, budget constraints, and considerations related to privacy and legal regulations. Additionally, advancements in camera technology, such as higher-resolution cameras and video analytics, may allow for more efficient coverage with fewer cameras.